

# Native Key Provider

Introduction, Design, and Operation

Bob Plankers

Cloud Infrastructure Security & Compliance, VMware

March 2023



# 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.



# Agenda

Data-at-Rest Encryption Features  
Features and concepts

Introduction to Native Key Provider  
KEKs, KDKs, DEKs, and more

Resources

Links to Cloud Infrastructure security materials

Questions + Answers

Real questions with real answers

# Data-at-Rest Encryption Features

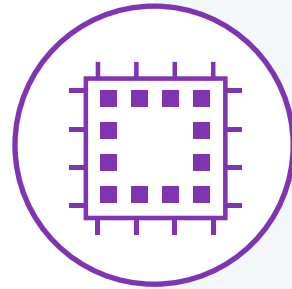


# Data-at-Rest Encryption in vSphere



## VM Encryption

Encrypts virtual machines on the storage they have. Can be everything or selective, choosing configuration files and/or individual VMDKs.



## vTPM

Virtual Trusted Platform Module (TPM), presenting a TPM 2.0 compatible device to the guest. Requires VM Encryption.



## vSAN Encryption

Encryption for entire vSAN datastores, seamlessly underneath VMs. Can be used by itself or in conjunction with VM Encryption.

# Your choice of Key Providers

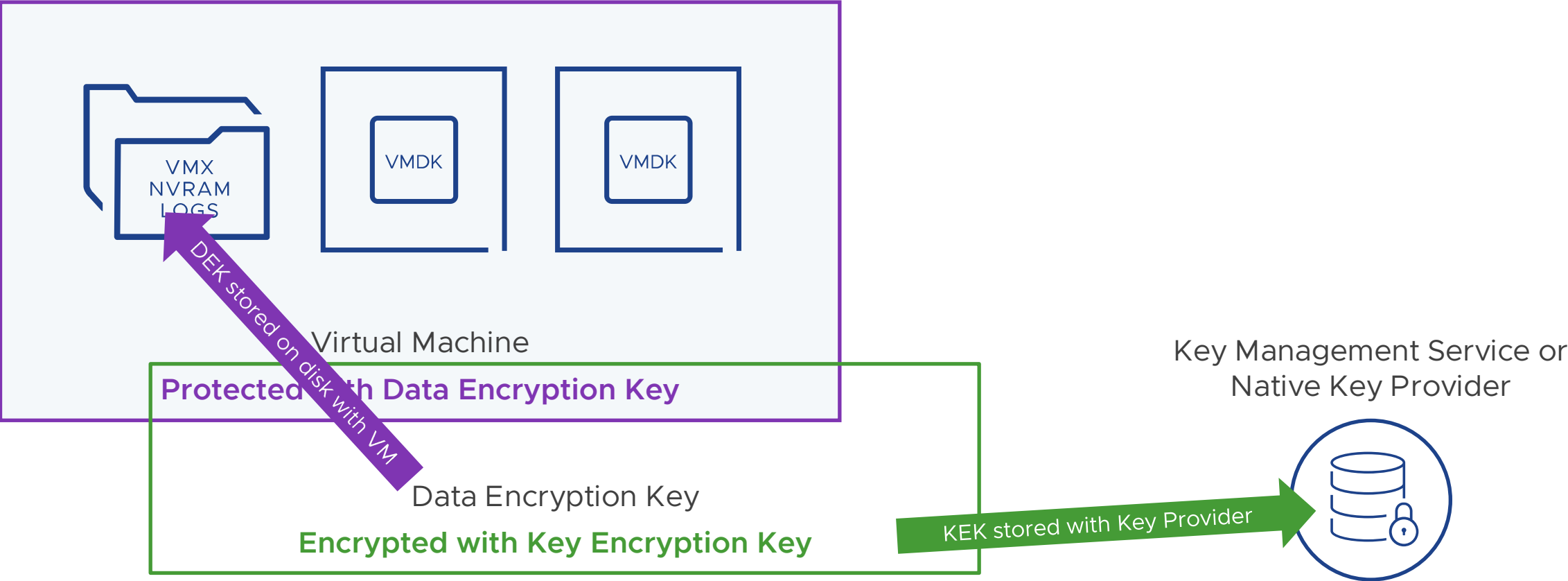


## Native Key Provider

vSphere and VMware Cloud on AWS can take advantage of the built-in Native Key Provider functionality, making it easy to start encrypting.

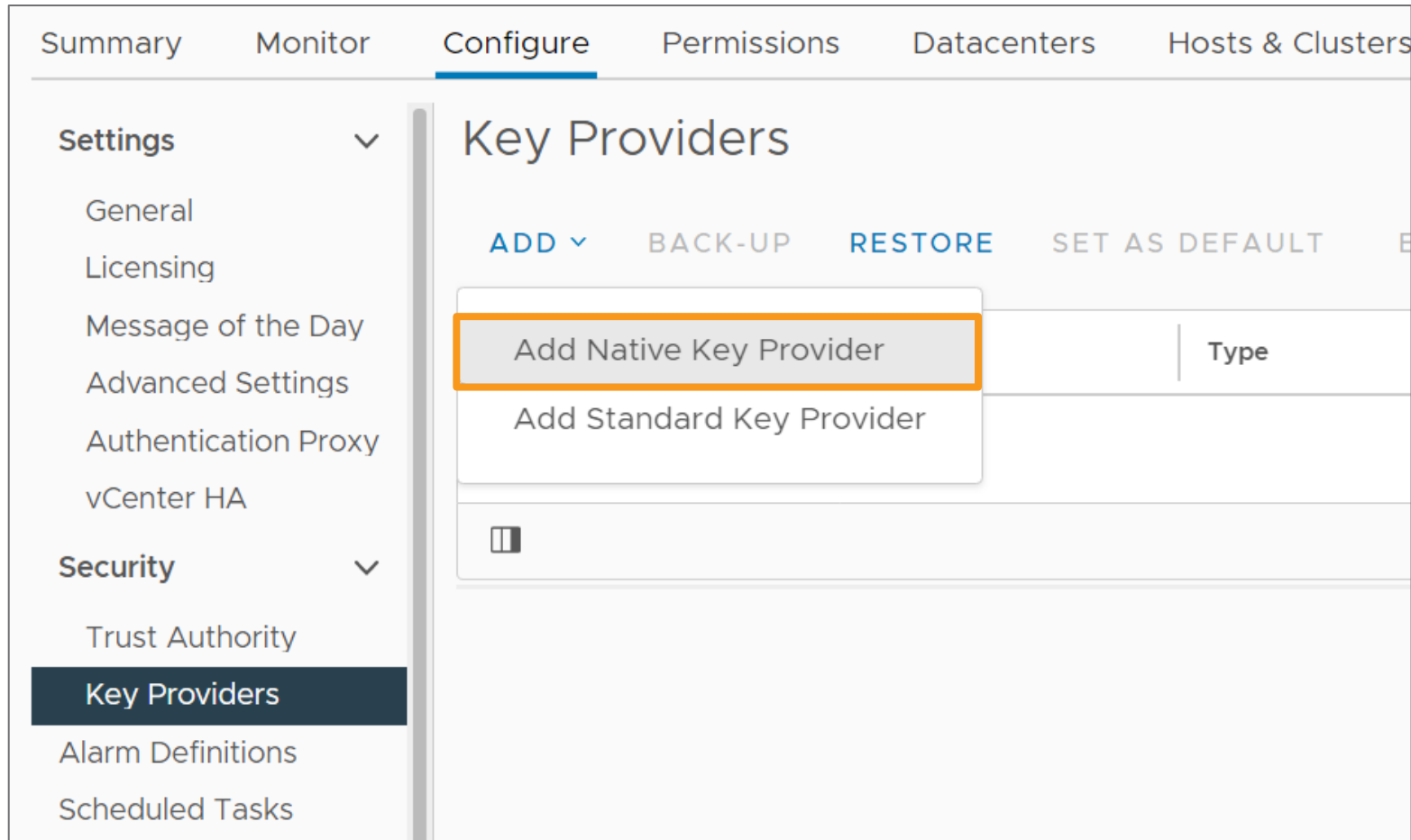
# Key Encryption Key vs. Data Encryption Key

## VM Encryption in vSphere



# Using Built-in Key Management from Native Key Provider (NKP)

## Native Key Provider in vSphere



### Considerations

- Only serves vSphere clusters
- Hosts will have Key Derivation Keys on them (but can use TPM)
- Hosts must be inside a cluster object in vCenter Server

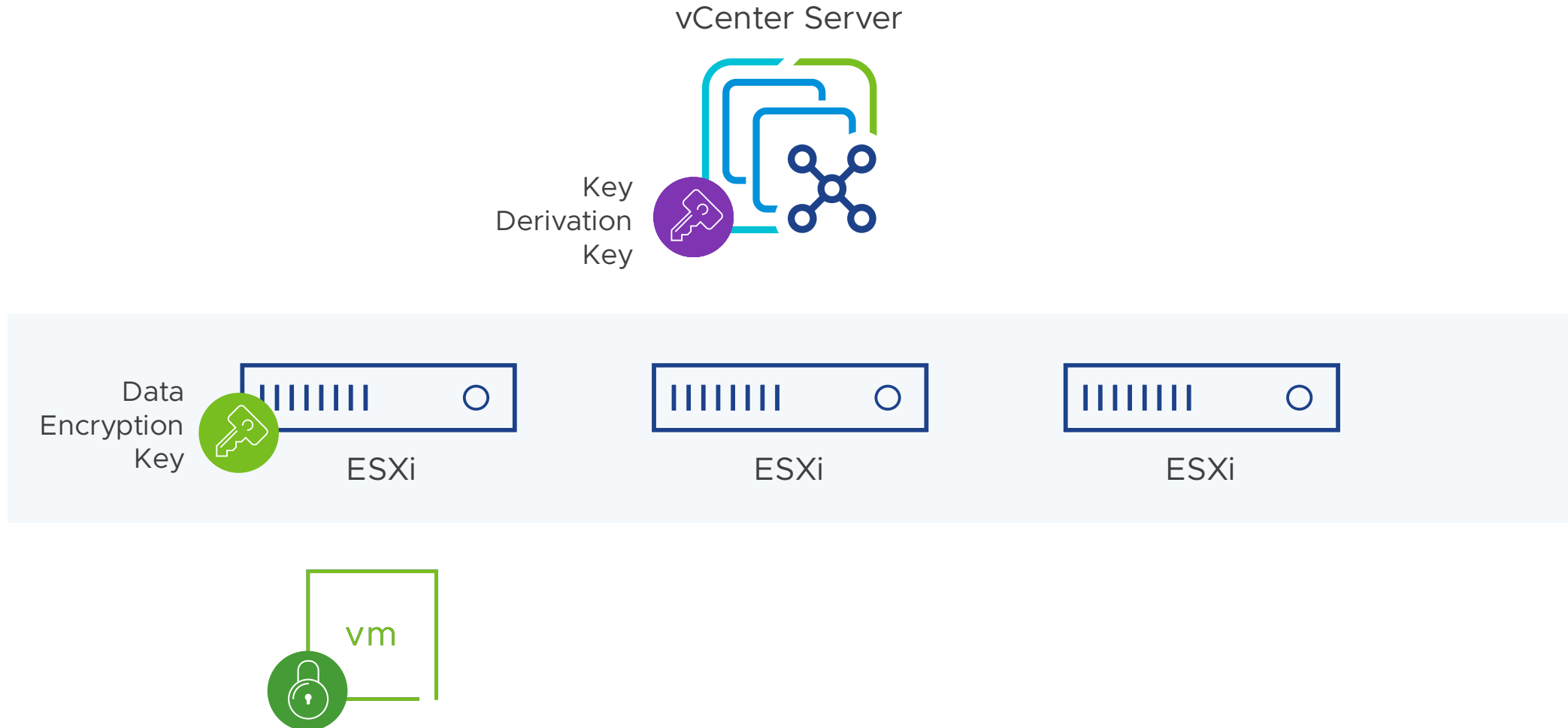
### Benefits

- Extremely easy to enable VM & vSAN encryption, and vTPM
- Helps prevent writing in clear to SSD, NVMe, flash devices
- Flexible, can convert to & from other key providers (shallow rekey)



# How VM Encryption & vTPM Work with Native Key Provider

## Native Key Provider in vSphere





vcenter-1.7.fcotr.org

ACTIONS

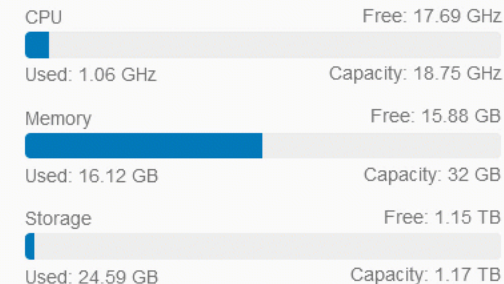
- ▼ vcenter-1.7.fcotr.org
  - ▼ Datacenter
    - ▼ vTA-A
      - esx-1.7.fcotr.org
      - esx-2.7.fcotr.org
      - esx-3.7.fcotr.org
      - esx-4.7.fcotr.org

- Summary
- Monitor
- Configure
- Permissions
- Datacenters
- Hosts & Clusters
- VMs
- Datastores
- Networks



Version: 7.0.2  
 Build: 18455184  
 Last Updated: Sep 23, 2021, 10:21 PM  
 Last File-Based Backup: [Not scheduled](#)

Clusters: 1  
 Hosts: 4  
 Virtual Machines: 3



Custom Attributes

Attribute	Value
No items to display	

[Edit...](#)

Tags

Health Status

Overall Health ✔ Good

APPLIANCE MANAGEMENT

vCenter HA

Mode --

State --

[Settings](#)



vcenter-1.7.fcotr.org

Datacenter

vTA-A

esx-1.7.fcotr.org

esx-2.7.fcotr.org

esx-3.7.fcotr.org

esx-4.7.fcotr.org

SECURE-VM-1

# SECURE-VM-1



ACTIONS

Summary

Monitor

Configure

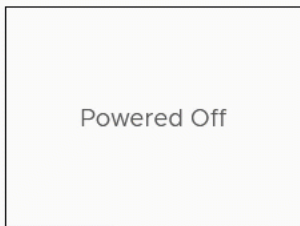
Permissions

Datastores

Networks

Snapshots

Updates



Powered Off

Guest OS: Microsoft Windows Server 2019 (64-bit)

Compatibility: ESXi 7.0 U2 and later (VM version 19)

VMware Tools: Not running, not installed

MORE INFO

DNS Name:

IP Addresses:

Host: esx-2.7.fcotr.org

LAUNCH WEB CONSOLE

LAUNCH REMOTE CONSOLE



SWITCH TO NEW VIEW



CPU USAGE

0 Hz



MEMORY USAGE

0 B



STORAGE USAGE

252 MB

## VM Hardware

> CPU	2 CPU(s)
> Memory	4 GB, 0 GB memory active
> Hard disk 1	90 GB
> Network adapter 1	1100-FCOTR-Mgmt-VTA (disconnected)
CD/DVD drive 1	Disconnected
> Video card	8 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface

## Notes

Edit Notes...

## Custom Attributes

Attribute	Value

Key Providers

### Add Native Key Provider



Bad name! Avoid a possible name collision by using a more unique name.

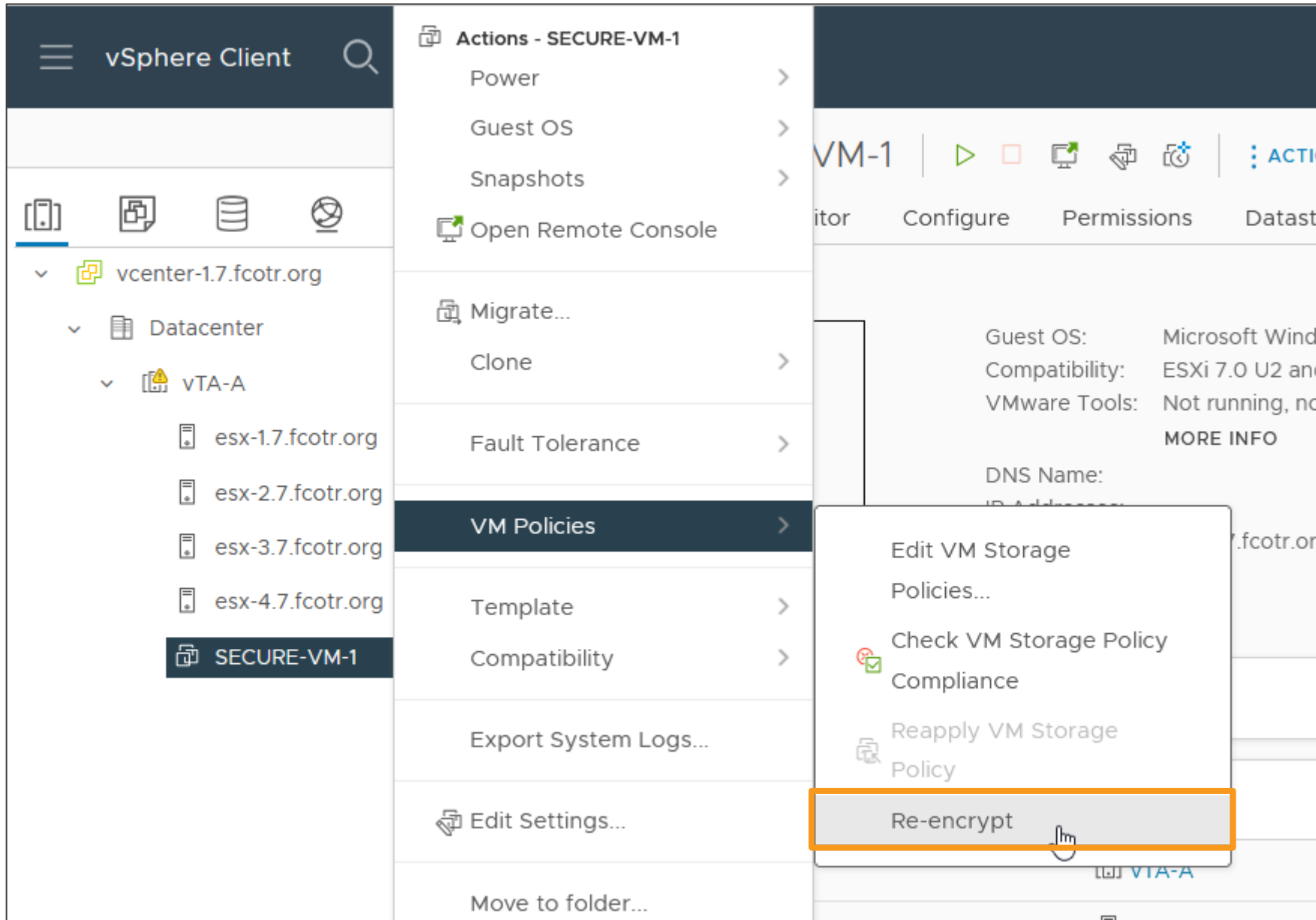
Name

Built-in

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

CANCEL

ADD KEY PROVIDER



Key Providers

## Add Native Key Provider



Name

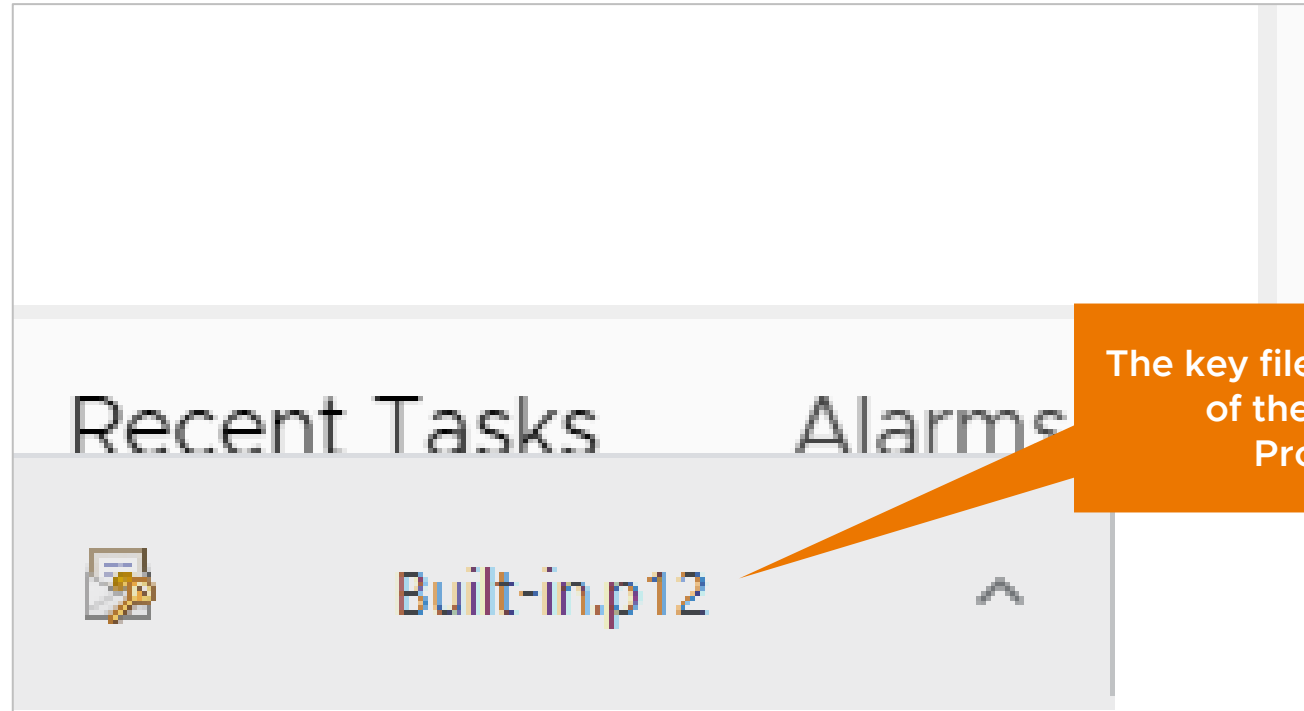
Built

Should you check this?!

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

CANCEL

ADD KEY PROVIDER



The key file will have the name of the key provider.  
Protect it well!

# Important: Configure & Secure vCenter Server Backups!

### Create Backup Schedule

Backup location ⓘ

Backup server credentials

User name

Password

Schedule ⓘ   :  P.M.

Encrypt backup (optional)

Encryption Password

Confirm Password

DB Health Check ⓘ  Enabled

Number of backups to retain

Retain all backups

Retain last  backups

Data

Stats, Events, and Tasks

Inventory and configuration  77 MB

Total size (compressed) 77 MB

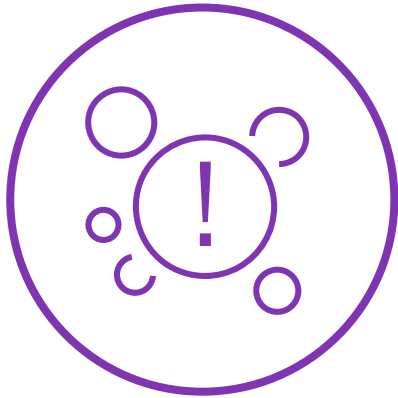


One NKP instance for everything?

**OR**

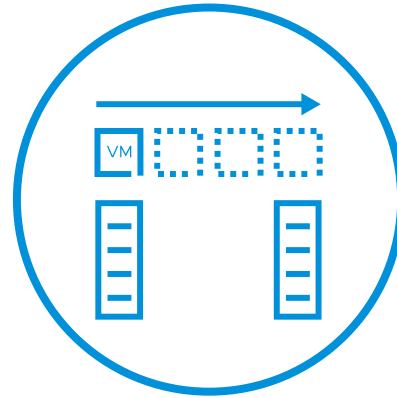
Individual NKP instances?

# Other Design Considerations for Native Key Provider



## Not a KMS

Different functionality,  
different guarantees



## Rekey Differences

Cannot rekey during  
migration or cloning



## Keys are Local

If the host is stolen the  
data can be accessed

# Which Key Provider Should You Choose?

Native Key Provider vs. Standard Key Provider

## Native Key Provider

---

Included in all VMware vSphere 7+ licenses

## Standard Key Provider

---

Requires a third-party Key Management System that permits KMIP connectivity

# Which Key Provider Should You Choose?

Native Key Provider vs. Standard Key Provider

## Native Key Provider

---

Included in all VMware vSphere 7+ licenses

Only serves VMware vSphere

## Standard Key Provider

---

Requires a third-party Key Management System that permits KMIP connectivity

Potential to connect other devices & systems

# Which Key Provider Should You Choose?

Native Key Provider vs. Standard Key Provider

## Native Key Provider

---

Included in all VMware vSphere 7+ licenses

Only serves VMware vSphere

Works with vSAN, VM Encryption, and vTPM

## Standard Key Provider

---

Requires a third-party Key Management System that permits KMIP connectivity

Potential to connect other devices & systems

Works with vSAN, VM Encryption, and vTPM

# Which Key Provider Should You Choose?

## Native Key Provider vs. Standard Key Provider

### Native Key Provider

---

Included in all VMware vSphere 7+ licenses

Only serves VMware vSphere

Works with vSAN, VM Encryption, and vTPM

Designed to avoid dependency loops with vCenter Server hosted inside the cluster

### Standard Key Provider

---

Requires a third-party Key Management System that permits KMIP connectivity

Potential to connect other devices & systems

Works with vSAN, VM Encryption, and vTPM

Requires design effort to mitigate dependencies and loops

# Which Key Provider Should You Choose?

## Native Key Provider vs. Standard Key Provider

### Native Key Provider

---

Included in all VMware vSphere 7+ licenses

Only serves VMware vSphere

Works with vSAN, VM Encryption, and vTPM

Designed to avoid dependency loops with vCenter Server hosted inside the cluster

All hosts participate & can decrypt directly

### Standard Key Provider

---

Requires a third-party Key Management System that permits KMIP connectivity

Potential to connect other devices & systems

Works with vSAN, VM Encryption, and vTPM

Requires design effort to mitigate dependencies and loops

VM Encryption proxied via vCenter Server  
vSAN Encryption speaks directly to KMS

# Which Key Provider Should You Choose?

## Native Key Provider vs. Standard Key Provider

### Native Key Provider

---

Included in all VMware vSphere 7+ licenses

Only serves VMware vSphere

Works with vSAN, VM Encryption, and vTPM

Designed to avoid dependency loops with vCenter Server hosted inside the cluster

All hosts participate & can decrypt directly

Cannot rotate keys while cloning VMs

### Standard Key Provider

---

Requires a third-party Key Management System that permits KMIP connectivity

Potential to connect other devices & systems

Works with vSAN, VM Encryption, and vTPM

Requires design effort to mitigate dependencies and loops

VM Encryption proxied via vCenter Server  
vSAN Encryption speaks directly to KMS

Can rotate keys while cloning



# Which Key Provider Should You Choose?

## Native Key Provider vs. Standard Key Provider

### Native Key Provider

---

Included in all VMware vSphere 7+ licenses

Only serves VMware vSphere

Works with vSAN, VM Encryption, and vTPM

Designed to avoid dependency loops with vCenter Server hosted inside the cluster

All hosts participate & can decrypt directly

Cannot rotate keys while cloning VMs

Stores decryption keys (KDK) on hosts

### Standard Key Provider

---

Requires a third-party Key Management System that permits KMIP connectivity

Potential to connect other devices & systems

Works with vSAN, VM Encryption, and vTPM

Requires design effort to mitigate dependencies and loops

VM Encryption proxied via vCenter Server  
vSAN Encryption speaks directly to KMS

Can rotate keys while cloning

KEKs only cached in host memory

# Which Key Provider Should You Choose?

## Native Key Provider vs. Standard Key Provider

### Native Key Provider

---

Included in all VMware vSphere 7+ licenses

Only serves VMware

Works with vSAN, V

Designed to avoid de

vCenter Server hosted

All hosts participate

Cannot rotate keys while cloning VMs

Stores decryption keys (KDK) on hosts

### Standard Key Provider

---

Requires a third-party Key Management System that permits KMIP connectivity

Capable to connect other devices & systems

Works with vSAN, VM Encryption, and vTPM

Requires design effort to mitigate

dependencies and loops

Encryption proxied via vCenter Server

vSAN Encryption speaks directly to KMS

Can rotate keys while cloning

KEKs only cached in host memory

If the attacker steals an NKP-enabled host, they can start an encrypted workload and/or access encrypted vSAN datastores

# Which Key Provider Should You Choose?

## Native Key Provider vs. Standard Key Provider

### Native Key Provider

---

Included in all VMware vSphere 7+ licenses

Only serves VMware vSphere

Works with vSAN, VM Encryption, and vTPM

Designed to avoid dependency loops with vCenter Server hosted inside the cluster

All hosts participate & can decrypt directly

Cannot rotate keys while cloning VMs

Stores decryption keys (KDK) on hosts

### Standard Key Provider

---

Requires a third-party Key Management System that permits KMIP connectivity

Potential

Works w

Requires  
depend

VM Enc

vSAN Encryption links directly to KMS

Can rotate keys while cloning

KEKs only cached in host memory

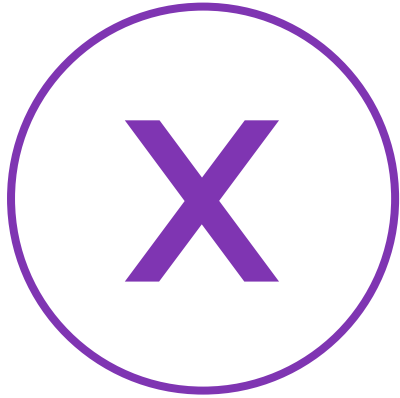
If the host loses power, it will lose all cached KEKs, and will need to connect to the KMS again at boot

“Can’t you do something about that?!”



What about  
system  
hardening?!

“Can’t you do something about that?!”

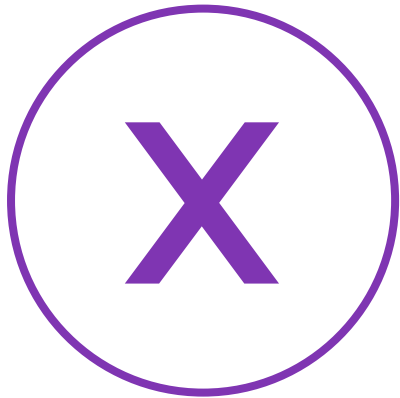


What about  
system  
hardening?!



We can't have  
a network  
dependency!

“Can’t you do something about that?!”



What about  
system  
hardening?!

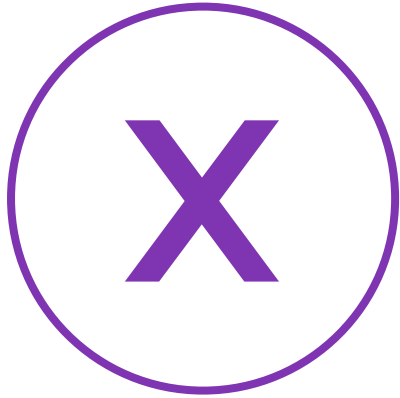


We can't have  
a network  
dependency!



We'll add a  
TPM!

“Can’t you do something about that?!”



What about  
system  
hardening?!



We can't have  
a network  
dependency!



We'll add a  
TPM!



We'll put  
vCenter Server  
in a central DC!

“Can’t you do something about that?!”



What about system hardening?!



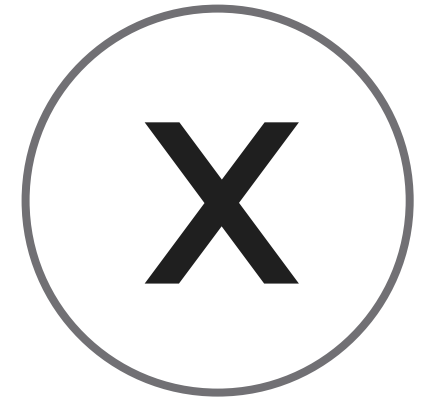
We can't have a network dependency!



We'll add a TPM!



We'll put vCenter Server in a central DC!

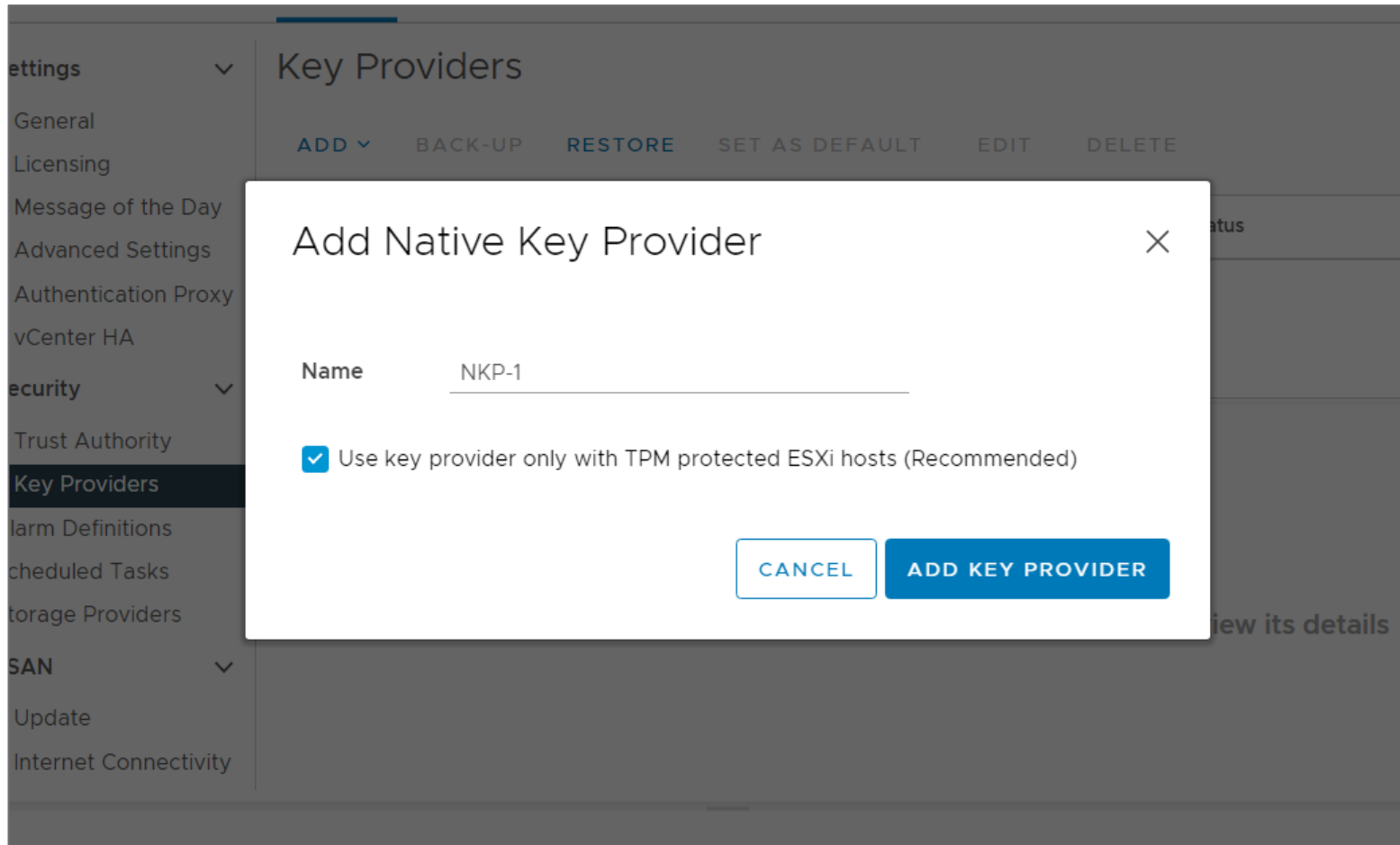


The feature needs to be enhanced!



# Recap: Native Key Provider

## Best Practices & Design Ideas for Native Key Provider in vSphere



### Lose the keys, lose your data: save the backup key

Can export & import keys between vCenter Servers for replication and other needs

Choose the Key Provider name well, you may need to import it elsewhere

Secure vCenter Server file-based backup & restore

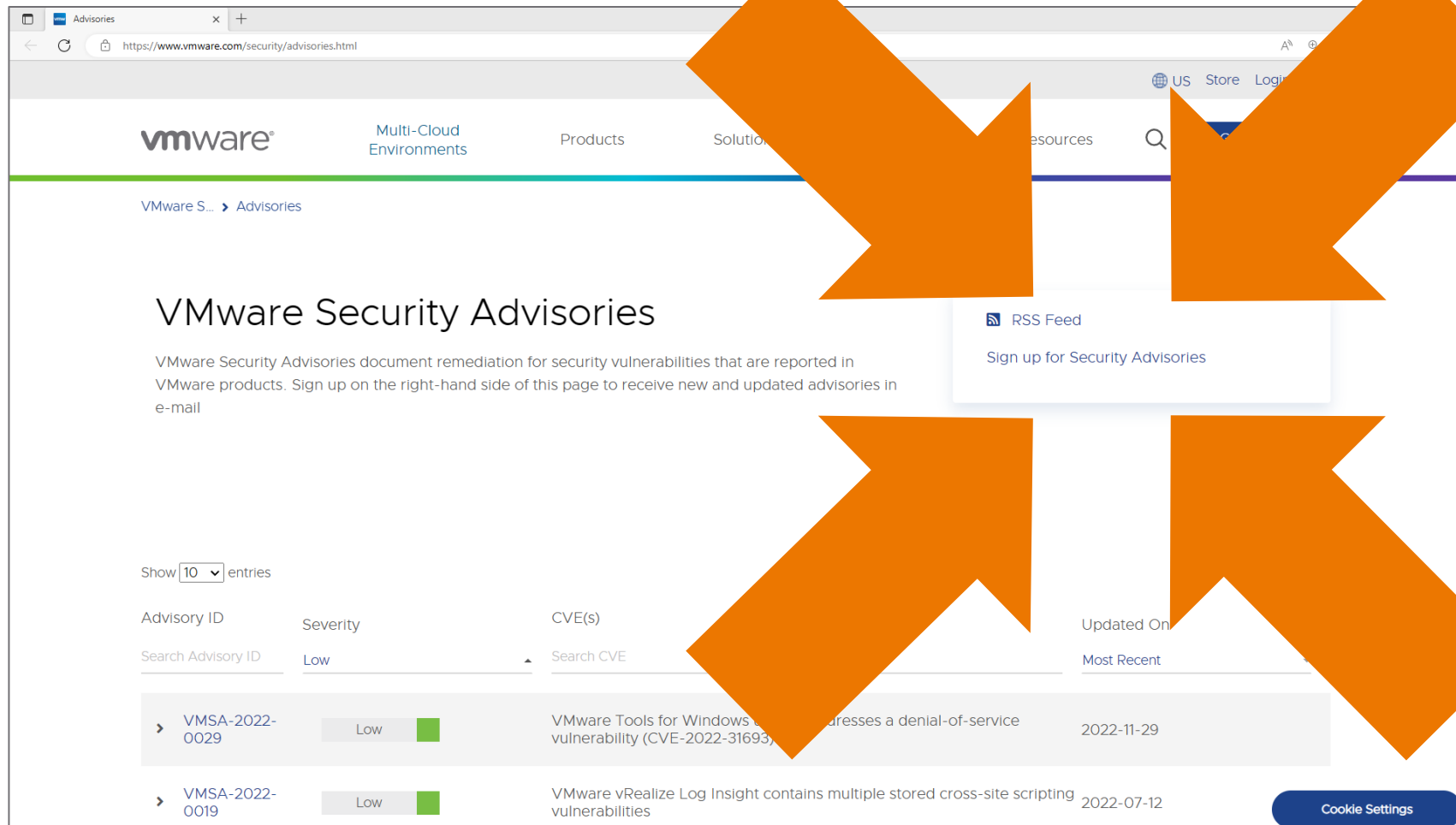
Mind the physical security of your hosts!

# Resources



# Sign Up For VMware Security Advisory (VMSA) Email

<https://www.vmware.com/security/advisories.html>



The screenshot shows the VMware Security Advisories page. The page title is "VMware Security Advisories". Below the title, there is a paragraph: "VMware Security Advisories document remediation for security vulnerabilities that are reported in VMware products. Sign up on the right-hand side of this page to receive new and updated advisories in e-mail". On the right-hand side, there is a button labeled "Sign up for Security Advisories". Four large orange arrows are overlaid on the page, pointing towards this button. The page also features a table of advisories with columns for Advisory ID, Severity, CVE(s), and Updated On. The first entry is VMSA-2022-0029 with a severity of Low, updated on 2022-11-29. The second entry is VMSA-2022-0019 with a severity of Low, updated on 2022-07-12.

Advisory ID	Severity	CVE(s)	Updated On
VMSA-2022-0029	Low	VMware Tools for Windows addresses a denial-of-service vulnerability (CVE-2022-31693)	2022-11-29
VMSA-2022-0019	Low	VMware vRealize Log Insight contains multiple stored cross-site scripting vulnerabilities	2022-07-12

VMsAs emailed  
the moment  
they are  
published

Just VMSAs;  
no marketing

Know before  
your Infosec  
people ask!

Prevention is a  
matter of time

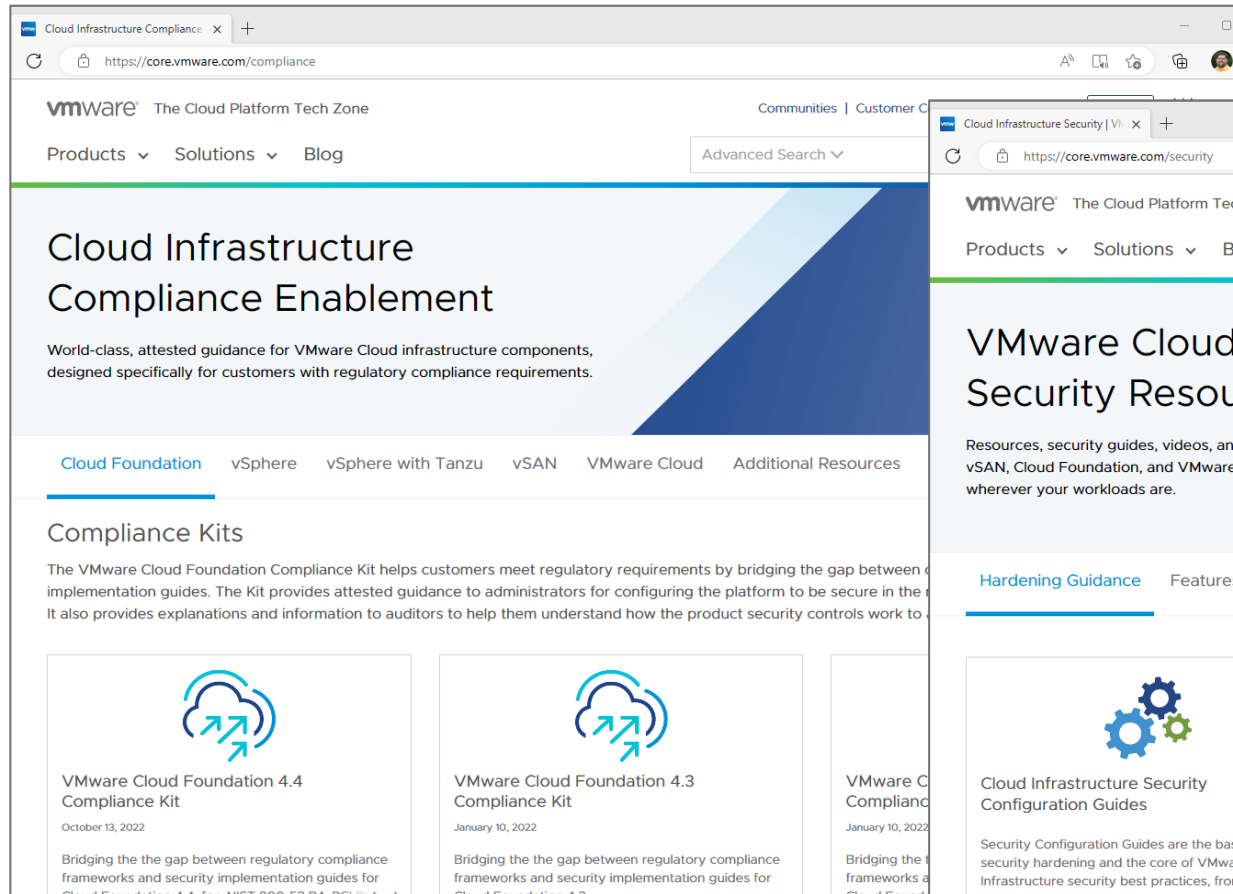
# VMware Cloud Infrastructure Security Configuration Guides

<https://via.vmw.com/scg>



# core.vmware.com

## Security & Compliance Resources for VMware Cloud Infrastructure



Cloud Infrastructure Compliance

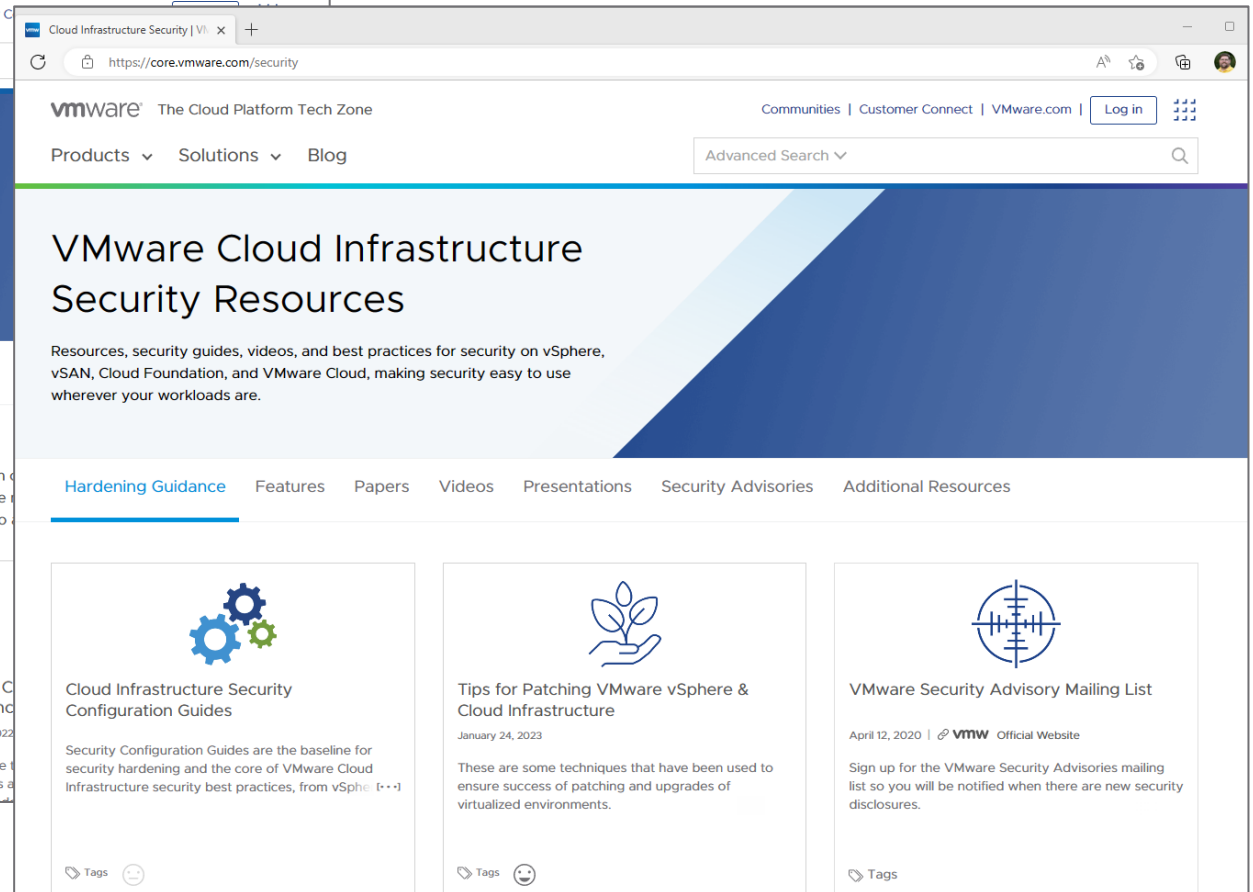
World-class, attested guidance for VMware Cloud infrastructure components, designed specifically for customers with regulatory compliance requirements.

Cloud Foundation | vSphere | vSphere with Tanzu | vSAN | VMware Cloud | Additional Resources

### Compliance Kits

The VMware Cloud Foundation Compliance Kit helps customers meet regulatory requirements by bridging the gap between implementation guides. The Kit provides attested guidance to administrators for configuring the platform to be secure in the cloud. It also provides explanations and information to auditors to help them understand how the product security controls work to protect your data.

- VMware Cloud Foundation 4.4 Compliance Kit**  
October 13, 2022  
Bridging the gap between regulatory compliance frameworks and security implementation guides for VMware Cloud Foundation 4.4 for NIST 800-53, PCI DSS, and ISO 27001.
- VMware Cloud Foundation 4.3 Compliance Kit**  
January 10, 2022  
Bridging the gap between regulatory compliance frameworks and security implementation guides for VMware Cloud Foundation 4.3.
- VMware Cloud Foundation 4.2 Compliance Kit**  
January 10, 2022  
Bridging the gap between regulatory compliance frameworks and security implementation guides for VMware Cloud Foundation 4.2.



VMware Cloud Infrastructure Security Resources

Resources, security guides, videos, and best practices for security on vSphere, vSAN, Cloud Foundation, and VMware Cloud, making security easy to use wherever your workloads are.

Hardening Guidance | Features | Papers | Videos | Presentations | Security Advisories | Additional Resources

- Cloud Infrastructure Security Configuration Guides**  
Security Configuration Guides are the baseline for security hardening and the core of VMware Cloud Infrastructure security best practices, from vSphere 6.7 to VMware Cloud Foundation 4.4.
- Tips for Patching VMware vSphere & Cloud Infrastructure**  
January 24, 2023  
These are some techniques that have been used to ensure success of patching and upgrades of virtualized environments.
- VMware Security Advisory Mailing List**  
April 12, 2020 | VMware Official Website  
Sign up for the VMware Security Advisories mailing list so you will be notified when there are new security disclosures.

# Questions & Answers



## vSphere Native Key Provider Questions & Answers (FAQ)

<https://via.vmw.com/nkp-faq>

