Virtual TPM (vTPM)

Introduction, Design, and Q&A

Bob Plankers
Cloud Infrastructure Security & Compliance, VMware

April 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 Virtual TPM (vTPM)

Workload-centric security tools

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

Standard Key Provider

vSphere can connect to a traditional Key Management System (KMS) that will store and manage encryption keys.

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.

Trusted Key Provider

vSphere Trust Authority allows organizations to establish a Trusted Computing Base and continuously attest their infrastructure security.

Introduction to Virtual TPM (vTPM)

vmware

Trusted Platform Module

[ˈtrʌstɪd ˈplætfɔːm ˈmɒdjuːl]

A Trusted Platform Module, or TPM, is a computer chip that can securely store artifacts such as passwords, certificates, or encryption keys, that are used to authenticate the platform. It can also generate random data, and store platform measurements to help ensure trustworthiness of the system.

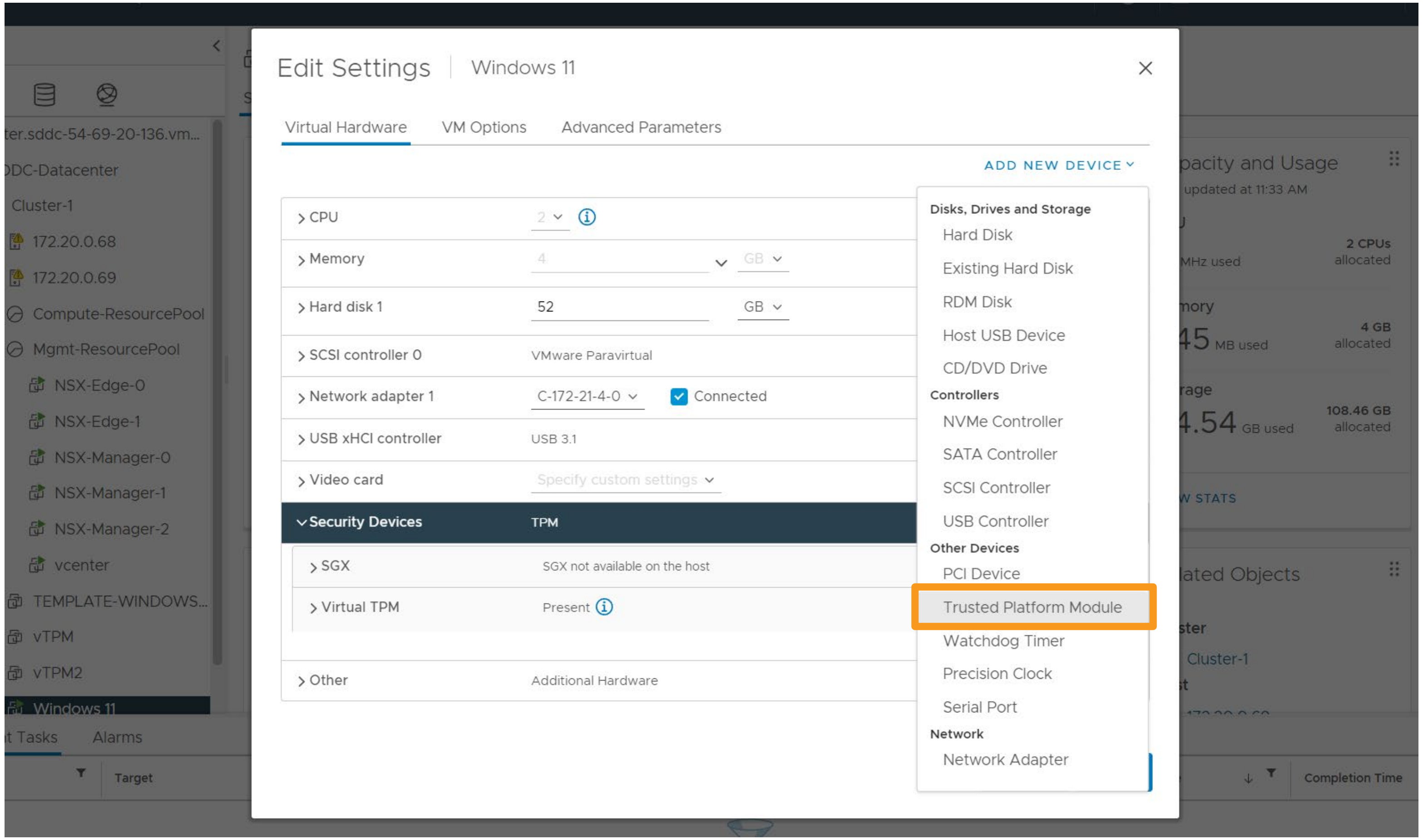
A **Hardware** Trusted Platform Module

Add these to your servers so ESXi can use them!

I belong to ESXi, not your workloads!

Workload Security & Compliance Made Easier

vTPM on VMware Cloud on AWS, vSphere, and Cloud Foundation



Edit Settings | Windows 11

Virtual Hardware | VM Options | Advanced Parameters

ADD NEW DEVICE

> CPU	2
> Memory	4 GB
> Hard disk 1	52 GB
> SCSI controller 0	VMware Paravirtual
> Network adapter 1	C-172-21-4-0 ☑ Connected
> USB xHCI controller	USB 3.1
> Video card	Specify custom settings
⌄ Security Devices	TPM
> SGX	SGX not available on the host
> Virtual TPM	Present
> Other	Additional Hardware

Considerations

Requires VM Encryption, so need a key provider configured

Cloning may also clone thevTPM

VM cannot be exported in encrypted form (OVF/OVA)

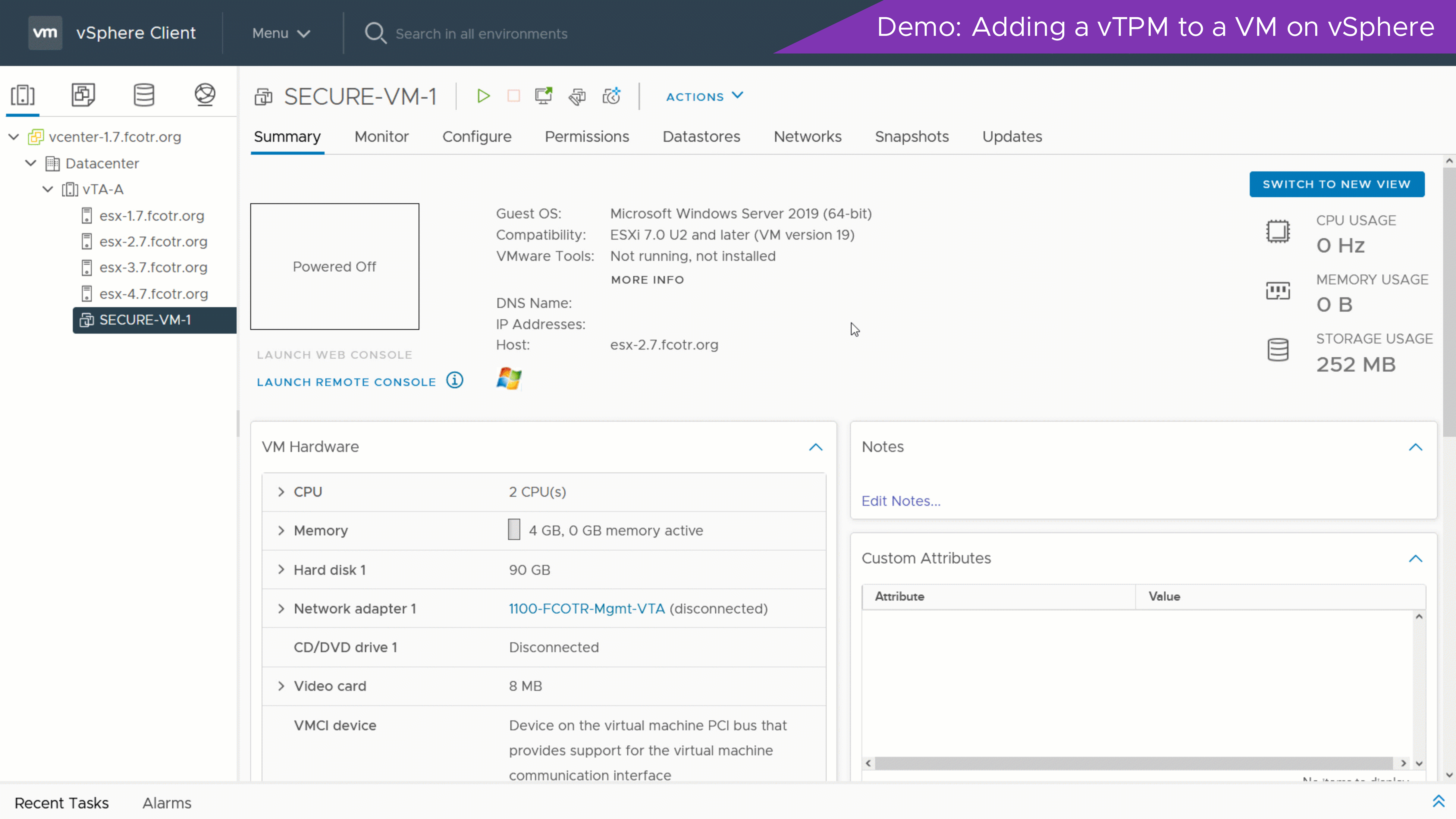
Benefits

Extremely easy to enable TPM functionality inside a workload

Native Key Provider and vTPM licensed for all vSphere versions

Does not depend on hardware TPM, at all, preserving vMotion

Demo: Adding a vTPM to a VM on vSphere



Guest OS: Microsoft Windows Server 2019 (64-bit)
Compatibility: ESXi 7.0 U2 and later (VM version 19)
VMware Tools: Not running, not installed
DNS Name:
IP Addresses:
Host: esx-2.7.fcotr.org

CPU USAGE 0 Hz
MEMORY USAGE 0 B
STORAGE USAGE 252 MB

VM Hardware

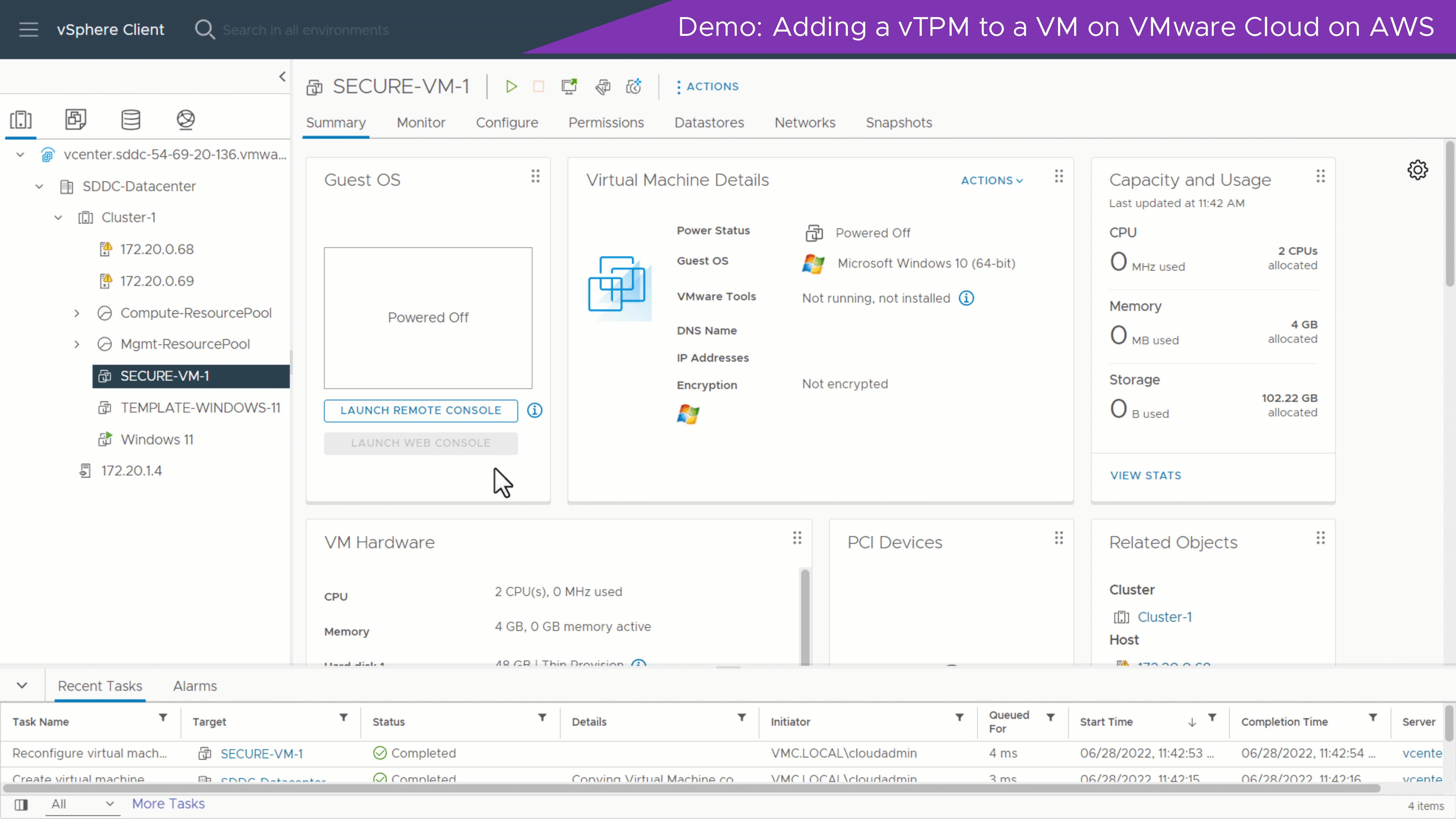
CPU	2 CPU(s)
Memory	4 GB, 0 GB memory active
Hard disk 1	90 GB
Network adapter 1	1100-FCOTR-Mgmt-VTA (disconnected)
CD/DVD drive 1	Disconnected
Video card	8 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface

Notes

Custom Attributes

Attribute	Value

Demo: Adding a vTPM to a VM on VMware Cloud on AWS



Guest OS

Powered Off

Virtual Machine Details

Power Status: Powered Off
Guest OS: Microsoft Windows 10 (64-bit)
VMware Tools: Not running, not installed
DNS Name:
IP Addresses:
Encryption: Not encrypted

Capacity and Usage
Last updated at 11:42 AM

CPU
0 MHz used
2 CPUs allocated

Memory
0 MB used
4 GB allocated

Storage
0 B used
102.22 GB allocated

VM Hardware

CPU: 2 CPU(s), 0 MHz used
Memory: 4 GB, 0 GB memory active
Hard disk 1: 48 GB | Thin Provision

PCI Devices

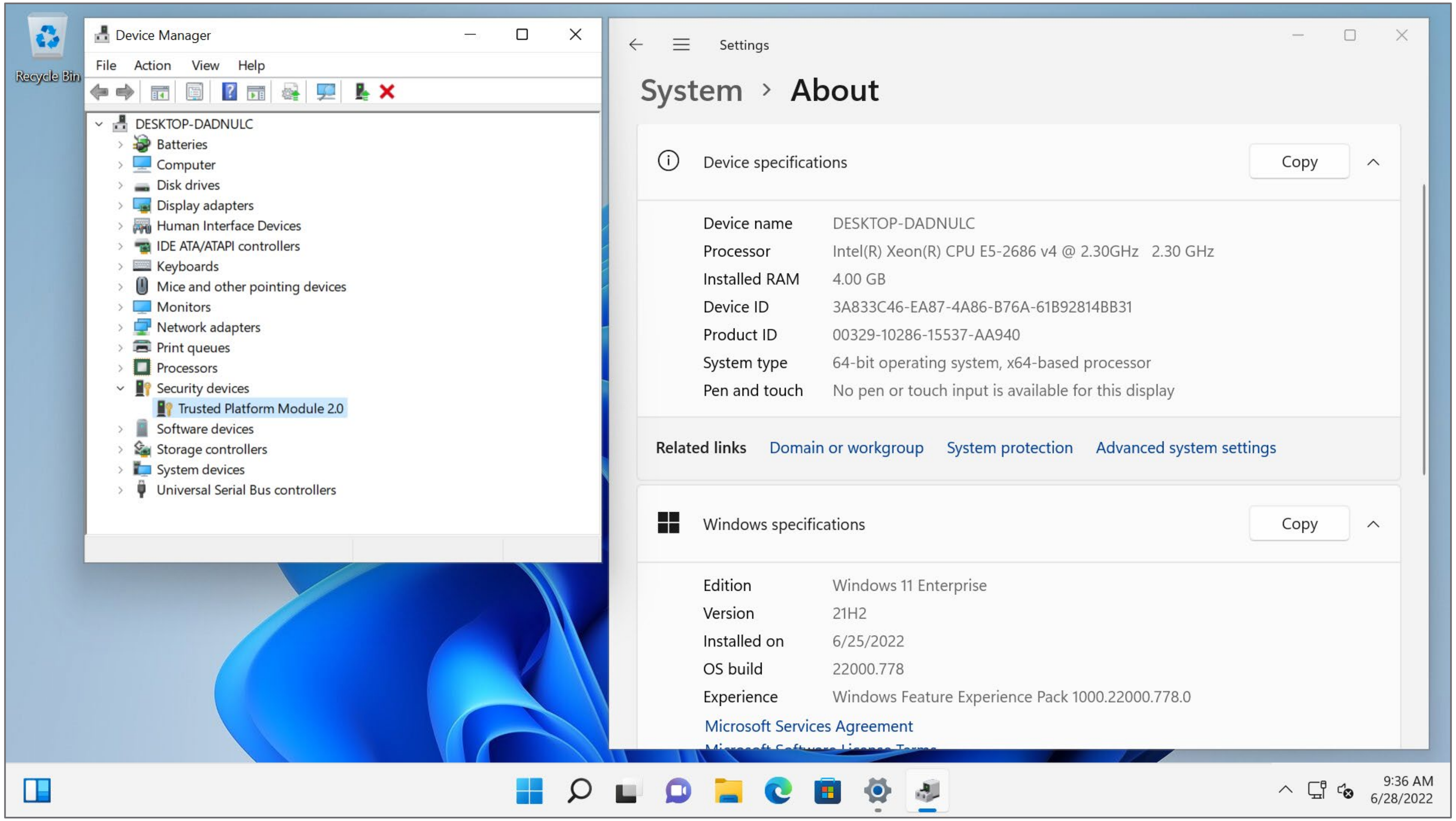
Related Objects

Cluster
Cluster-1
Host
172.20.0.68

Task Name	Target	Status	Details	Initiator	Queued For	Start Time	Completion Time	Server
Reconfigure virtual mach...	SECURE-VM-1	Completed		VMC.LOCAL\cloudadmin	4 ms	06/28/2022, 11:42:53 ...	06/28/2022, 11:42:54 ...	vcente
Create virtual machine	SDDC-Datacenter	Completed	Copying Virtual Machine co...	VMC.LOCAL\cloudadmin	3 ms	06/28/2022, 11:42:15	06/28/2022, 11:42:16	vcente

Windows 11 Works Well with vTPM

vTPM on VMware Cloud on AWS, vSphere, and Cloud Foundation



- DESKTOP-DADNULC
  - Batteries
  - Computer
  - Disk drives
  - Display adapters
  - Human Interface Devices
  - IDE ATA/ATAPI controllers
  - Keyboards
  - Mice and other pointing devices
  - Monitors
  - Network adapters
  - Print queues
  - Processors
  - Security devices
    - Trusted Platform Module 2.0
  - Software devices
  - Storage controllers
  - System devices
  - Universal Serial Bus controllers

System › About

Device specifications — Copy

Device name	DESKTOP-DADNULC
Processor	Intel(R) Xeon(R) CPU E5-2686 v4 @ 2.30GHz 2.30 GHz
Installed RAM	4.00 GB
Device ID	3A833C46-EA87-4A86-B76A-61B92814BB31
Product ID	00329-10286-15537-AA940
System type	64-bit operating system, x64-based processor
Pen and touch	No pen or touch input is available for this display

Related links Domain or workgroup System protection Advanced system settings

Windows specifications — Copy

Edition	Windows 11 Enterprise
Version	21H2
Installed on	6/25/2022
OS build	22000.778
Experience	Windows Feature Experience Pack 1000.22000.778.0

Microsoft Services Agreement

Microsoft Software License Terms

Meets hardware requirements for Windows 11

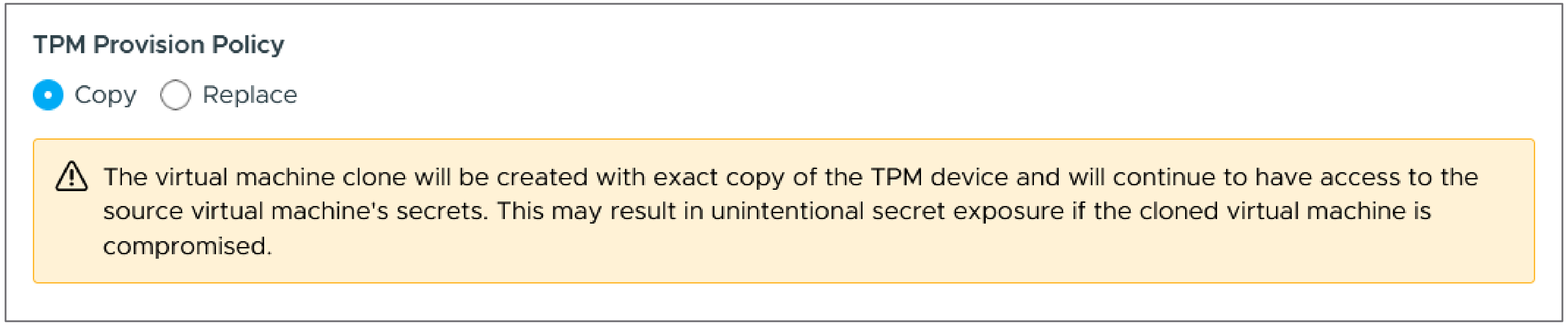
Supported by Microsoft on i3en+ instances in VMware Cloud on AWS

vTPM secures Bitlocker, Device Guard, Credential Guard, and more

vmware®

What About Cloning a VM?

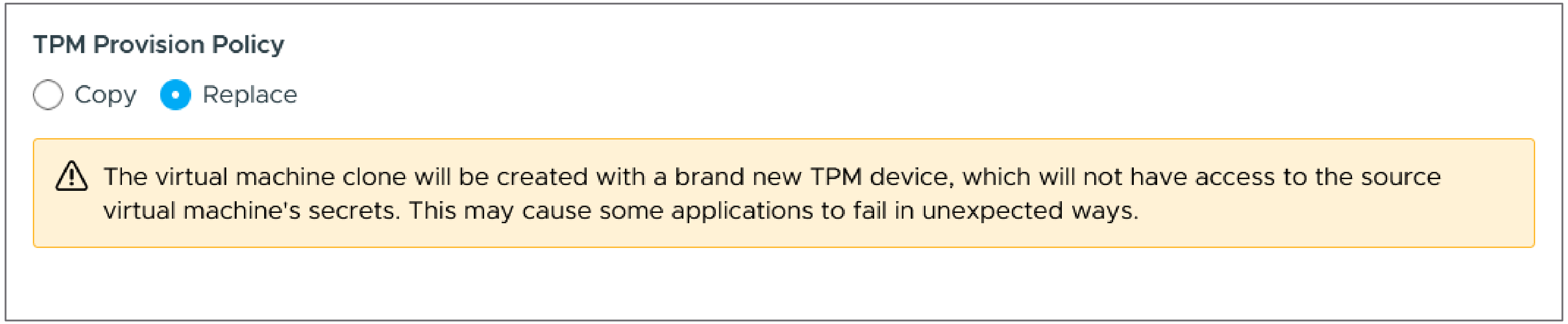
vTPM on VMware Cloud on AWS, vSphere, and Cloud Foundation



TPM Provision Policy

● Copy ○ Replace

⚠ The virtual machine clone will be created with exact copy of the TPM device and will continue to have access to the source virtual machine's secrets. This may result in unintentional secret exposure if the cloned virtual machine is compromised.



TPM Provision Policy

○ Copy ● Replace

⚠ The virtual machine clone will be created with a brand new TPM device, which will not have access to the source virtual machine's secrets. This may cause some applications to fail in unexpected ways.

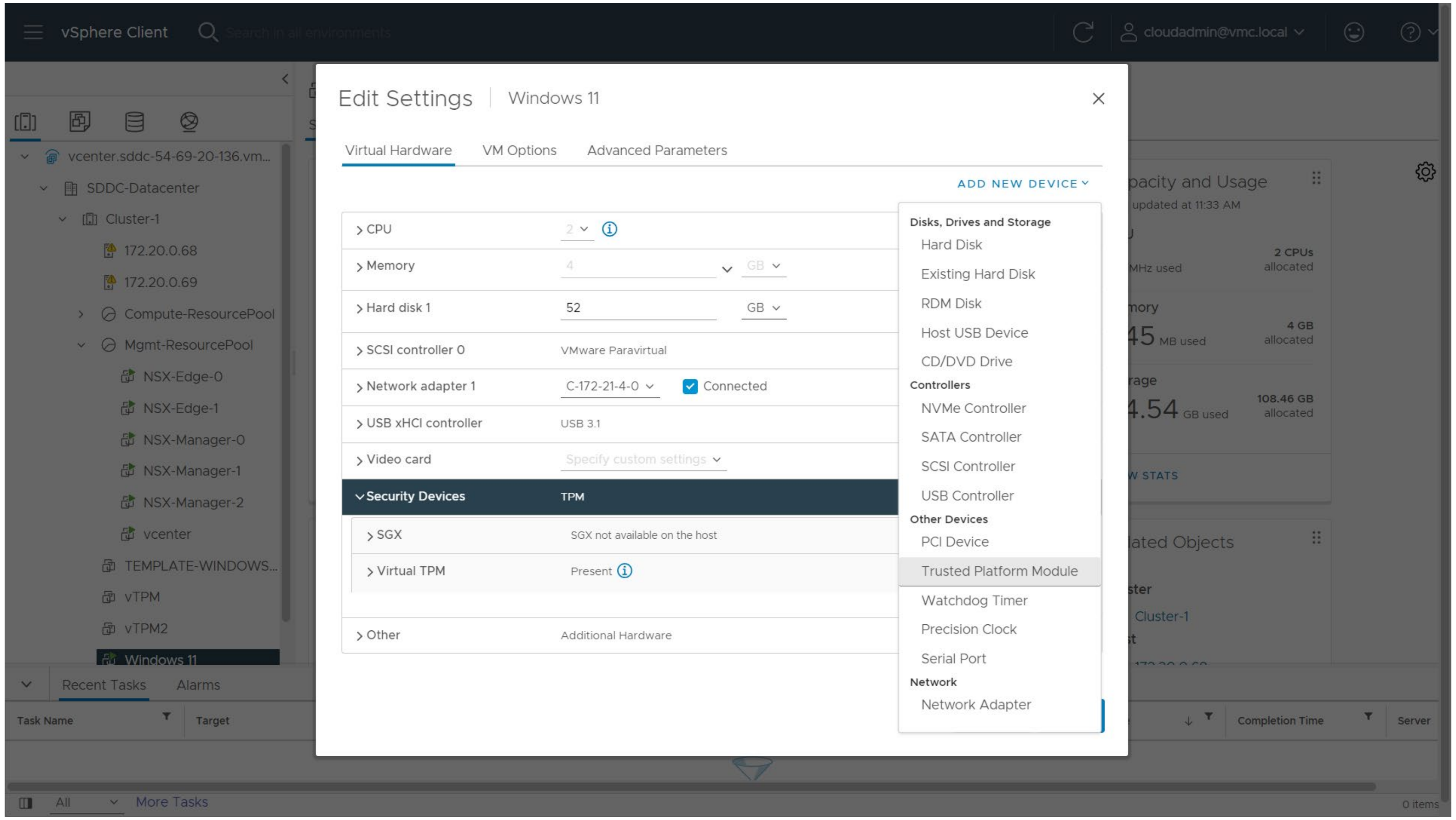
vSphere 6.7 and 7 will simply clone the VM, as-is, **an exact copy**

vSphere 8 offers **the choice to replace the TPM** with a new, blank version

Your choice based on what you intend to do!

Thoughts on using vTPM

Best Practices & Design Ideas for vTPM



Edit Settings | Windows 11

Virtual Hardware | VM Options | Advanced Parameters

- CPU: 2
- Memory: 4 GB
- Hard disk 1: 52 GB
- SCSI controller 0: VMware Paravirtual
- Network adapter 1: C-172-21-4-0 ☑ Connected
- USB xHCI controller: USB 3.1
- Video card: Specify custom settings
- Security Devices: TPM
  - SGX: SGX not available on the host
  - Virtual TPM: Present
- Other: Additional Hardware

Consider the cloning workflows based on the vSphere version

Addition of vTPM encrypts VM Home files, but not VMDKs

Encrypted VMs cannot be exported to OVF/OVA

Cross-vCenter vMotion is possible if the key provider is available in both places

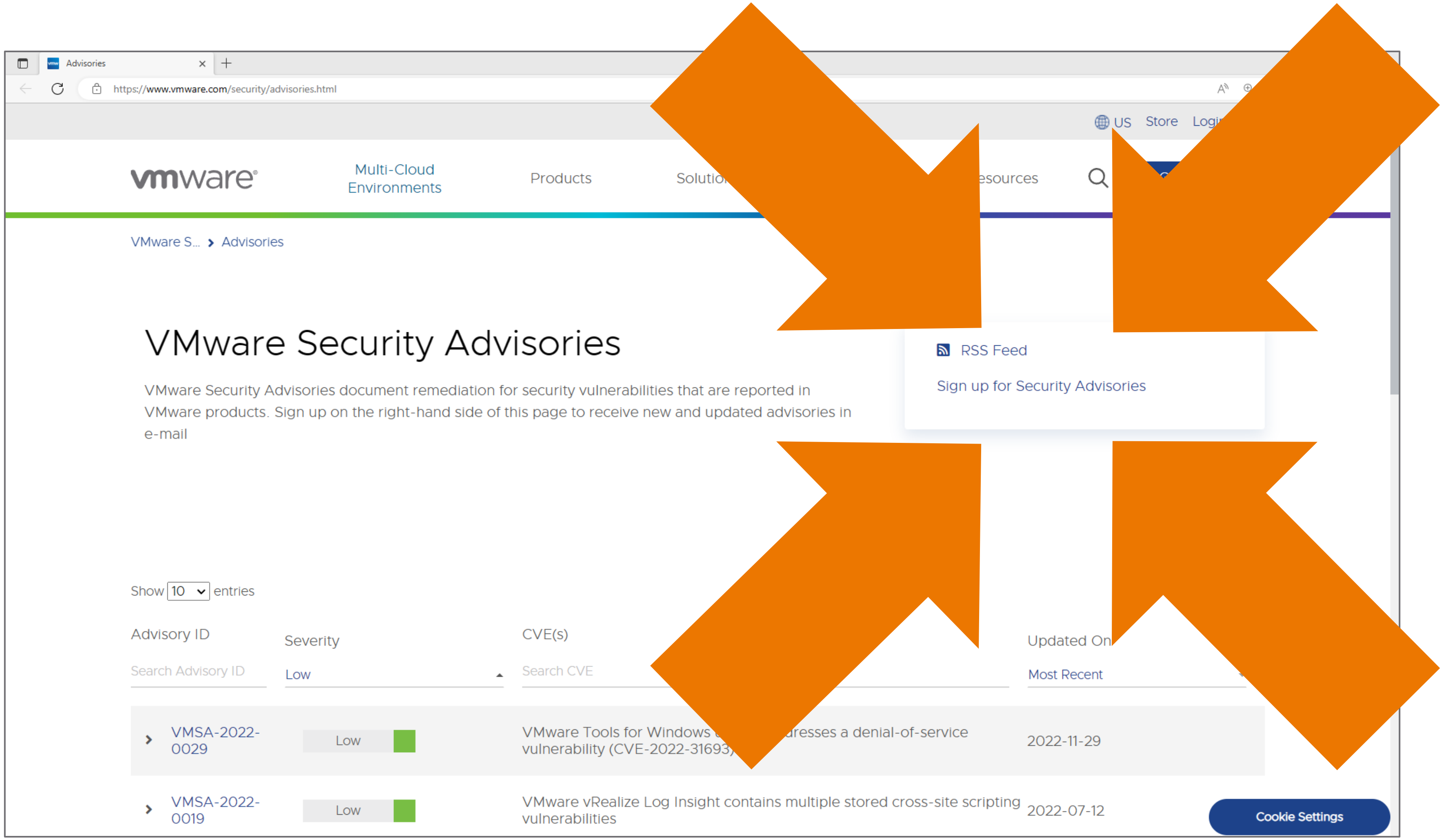
Requires VM to be configured with EFI firmware

VM must be powered off to add the device & encrypt home files

Resources

Sign Up For VMware Security Advisory (VMSA) Email

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



VMware Security Advisories

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

RSS Feed

Sign up for Security Advisories

Show 10 entries

Advisory ID	Severity	CVE(s)	Updated On
Search Advisory ID	Low	Search CVE	Most Recent
VMSA-2022-0029	Low	VMware Tools for Windows ddresses 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

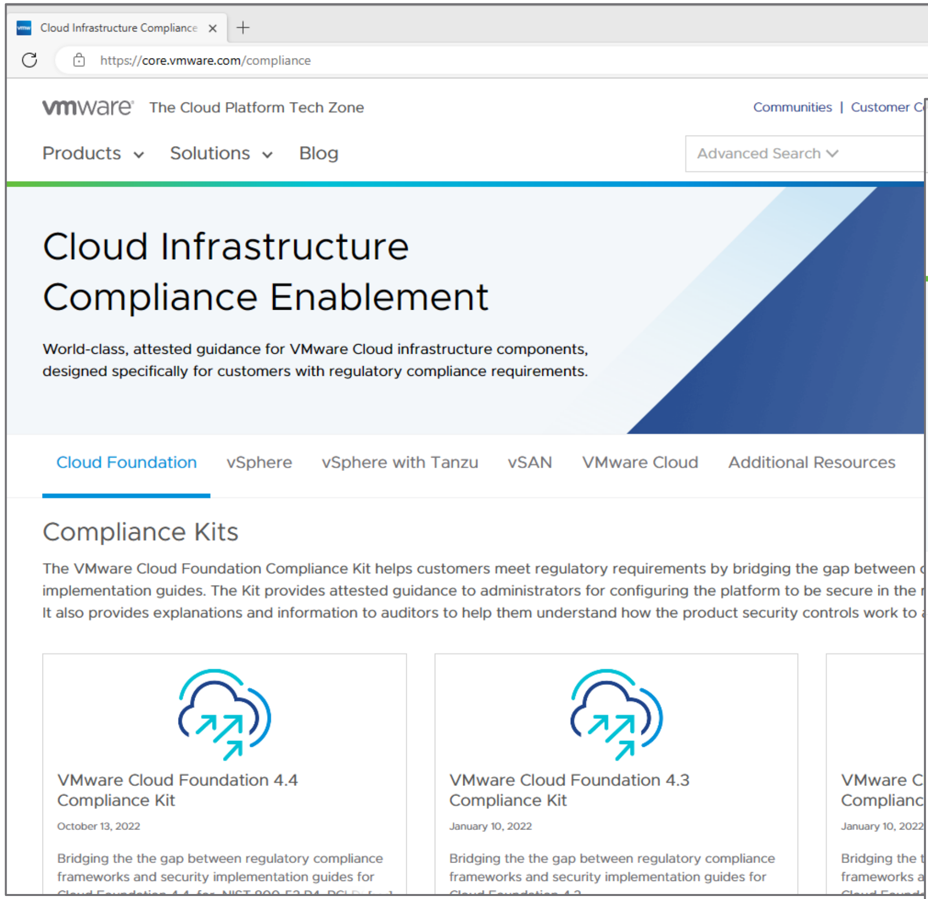
ADDITIONAL RESOURCES

VMware Cloud Infrastructure Security Configuration Guides

https://via.vmw.com/scg

core.vmware.com

Security & Compliance Resources for VMware Cloud Infrastructure


Cloud Infrastructure Compliance
https://core.vmware.com/compliance
vmware The Cloud Platform Tech Zone
Communities | Customer C
Products
Solutions
Blog
Advanced Search

Cloud Infrastructure Compliance Enablement

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

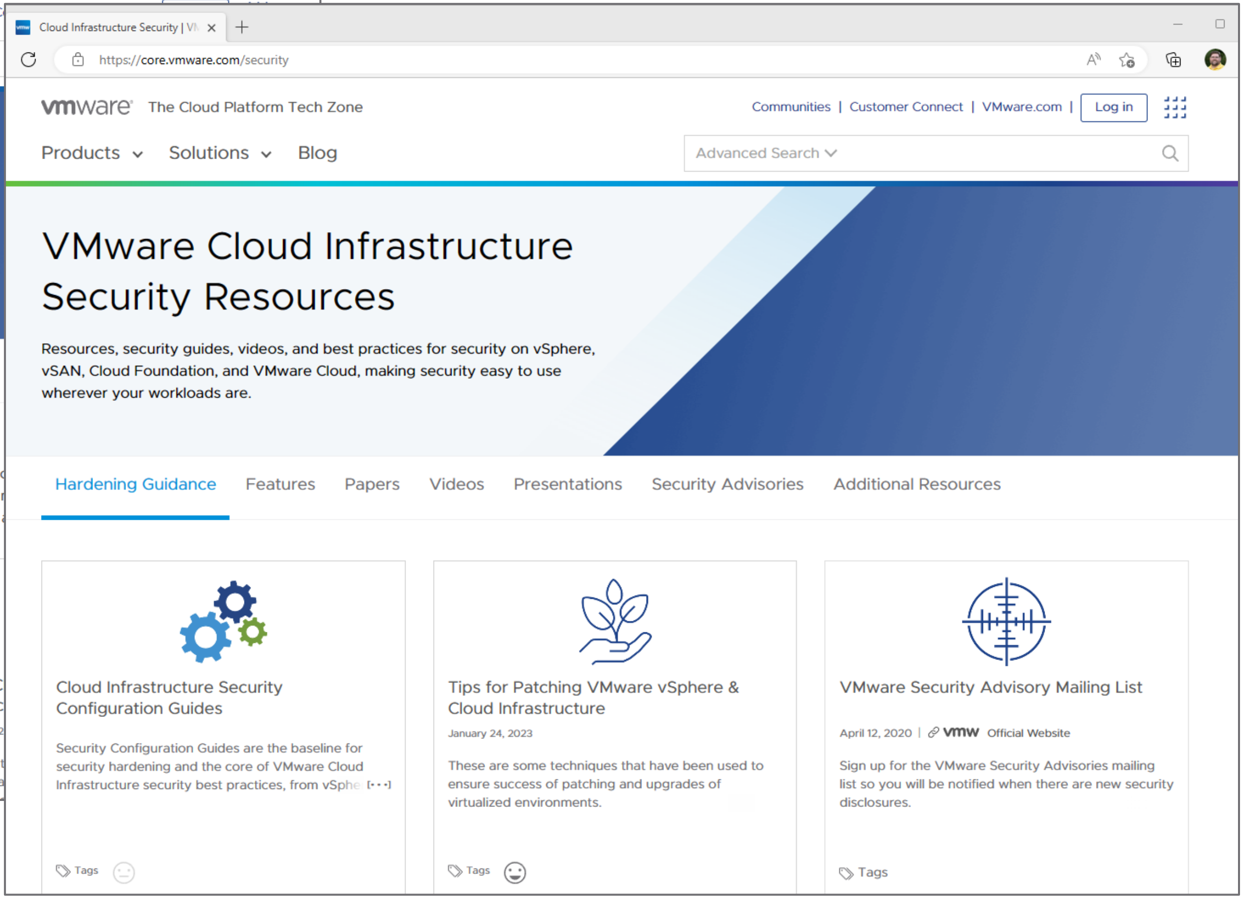
Compliance Kits

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

VMware Cloud Foundation 4.4 Compliance Kit
October 13, 2022
Bridging the the gap between regulatory compliance frameworks and security implementation guides for

VMware Cloud Foundation 4.3 Compliance Kit
January 10, 2022
Bridging the the gap between regulatory compliance frameworks and security implementation guides for

VMware C
Complianc
January 10, 2022
Bridging the t
frameworks a


Cloud Infrastructure Security | VI
https://core.vmware.com/security
vmware The Cloud Platform Tech Zone
Communities | Customer Connect | VMware.com | Log in
Products
Solutions
Blog
Advanced Search

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 vSphe [...]

Tags

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.

Tags

VMware Security Advisory Mailing List
April 12, 2020 | vmw Official Website

Sign up for the VMware Security Advisories mailing list so you will be notified when there are new security disclosures.

Tags

Questions & Answers

ADDITIONAL RESOURCES

vSphere vTPM
Questions & Answers (FAQ)

https://via.vmw.com/vtpm-faq