vTPM and Windows 11 on VMware Cloud on AWS

Table of contents

vTPM and Windows 11 on VMware Cloud on AWS

The release of VMware Cloud on AWS 1.19 (and future releases) adds support for virtual Trusted Platform Modules, or vTPMs. Trusted Platform Modules (TPMs) serve as cryptographic coprocessors for operating systems, helping the operating system do three major things:

- First, a TPM helps generate “randomness” in order to help operating systems do secure cryptography. Without random numbers and data, it is easier to predict encryption keys, which makes them susceptible to decoding by unauthorized people.
- Second, a TPM works with UEFI Secure Boot to record information about how the operating system started up. Another process can come along after the system starts up and review that information to determine if the system started securely or not, helping attest to the security of the system.
- Last, a TPM provides a secure enclave to store secrets, like encryption keys. TPMs seal data inside them and require proof from the operating system that it is authorized to unseal the information. This helps keep important data out of the hands of unauthorized people.

VMware Cloud on AWS 1.19 (and later) enables the use of virtual TPMs for workloads. These virtual TPMs are compliant with the TPM 2.0 specification and can be used seamlessly by virtual workloads that need the services of a TPM, just as if the workload were running directly on physical hardware.

vTPMs are backed by VM Encryption, helping to protect secrets that the vTPM stores. In turn, VM Encryption is backed by Native Key Provider, a feature that was added to vSphere 7 to make it easy to enable encryption in vSphere, vSAN, and now VMware Cloud.

vTPMs are supported on all manner of Linux and Windows guest operating systems, but one stands out: Microsoft Windows 11. When Windows 11 was released, Microsoft began requiring a TPM to install it. With a vTPM it is very easy to install Windows 11 in VMware Cloud on AWS, and our own staff architect, Bob Plankers, recorded himself walking through the whole process, from configuring the new VM to changing the pvscsi and vmxnet3 adapters:

Windows 11 isn’t the only Windows to benefit, though. The vTPM can be added to all supported Windows and Windows Server versions to help with regulatory compliance, like that of the DISA STIG.

vTPMs have a few considerations to them in VMware Cloud on AWS, things you should note as you consider how you can enable and use them:

- Virtual machine clones create full vTPM copies, which include the contents of the vTPM. If you are deploying new VMs you should incorporate removing and re-adding the vTPM into the workflow.
- The addition of vTPMs encrypts the VM home files, but not the VMDKs. vSAN data-at-rest encryption already protects the VMDKs in VMware Cloud on AWS.
- Native Key Provider is automatically set up for use in a VMware Cloud on AWS 1.19 (and later) SDDC and is not configurable by the cloudadmin@vmc.local accounts (or equivalent). This means that keys cannot be imported and exported at this time, potentially impacting VM exports, cross-vCenter vMotions, and replications.
- To configure a vTPM a VM must use EFI firmware and Secure Boot, and be powered off at the time the device is added.

For more information and access to VMware Cloud on AWS please contact your Technical Account Manager, Customer Success representative, or account team. Thank you!