Microsoft shares detailed instructions on how to meet Windows 11 TPM requirements when migrating virtual machines

Microsoft has published detailed guidance for IT administrators and system administrators on how to handle virtual trusted platform module (vTPM) certificates.

Microsoft has published detailed guidance for IT administrators and system administrators on how to handle virtual trusted platform module (vTPM) certificates. The company says this is important to understand and implement correctly, as guest operating systems like Windows 11 and Windows Server 2025 running on Hyper-V Gen 2 virtual machines can maintain full security features when moved between physical servers.

Microsoft has always maintained that Windows 11's system requirements, such as TPM 2.0, are designed to provide better security than Windows 10 by default. How it works, vTPM enables security features like BitLocker and Secure Boot inside virtual machines. However, Hyper-V binds each vTPM instance to two self-signed certificates on the local physical server. Microsoft warns that live migration and manual export of vTPM-enabled virtual machines can fail if the certificates are not transferred properly. This can be a major issue because it prevents organizations from migrating protected workloads.

Microsoft notes that Hyper-V hosts automatically generate two self-signed certificates—one encryption certificate and one signing certificate—for each vTPM-enabled Generation 2 virtual machine, and store them in the "Shielded VM Local Certificates" repository located under Certificates (Local Computer) > Personal in the Microsoft Management Console (MMC). These include:

1. Shielded VM Encryption Certificate (UntrustedGuardian)(Computer Name)
2. Shielded VM Signing Certificate (UntrustedGuardian)(Computer Name)

Both encryption and signing certificates have a default validity period of 10 years.

To migrate properly, Microsoft notes that administrators must export both certificates along with their private keys as PFX (Personal Information Exchange) files and import them into the same repository on the destination servers, thereby marking them as trusted.

The company has detailed the steps for exporting, importing, and updating (in case the certificate expires), and also provided the corresponding PowerShell commands. You can check out the full detailed post here on the Microsoft Tech Community website .