Virtual Machine Encryption

Updated on 03/10/2022

Selected product version: VMware vSphere 7.0

With vSphere Virtual Machine Encryption, you can encrypt your sensitive workloads in an even more secure way. Access to encryption keys can be made conditional to the ESXi host being in a trusted state.

Before you can start with virtual machine encryption tasks, you must set up a key provider. The following key provider types are available.

vSphere Key Providers

Key Provider	Description	For More Information
Standard key provider	Available in vSphere 6.5 and later, the standard key provider uses vCenter Server to request keys from an external key server. The key server generates and stores the keys, and passes them to vCenter Server for distribution.	See Configuring and Managing a Standard Key Provider.
Trusted key provider	Available in vSphere 7.0 and later, the vSphere Trust Authority trusted key provider makes access to the encryption keys conditional to the attestation state of a workload cluster. vSphere Trust Authority requires an external key server.	See vSphere Trust Authority.
VMware vSphere® Native Key Provider™	Available in vSphere 7.0 Update 2 and later, vSphere Native Key Provider is included in all vSphere editions and does not require an external key server.	See Configuring and Managing vSphere Native Key Provider.

Comparison of vSphere Key Providers

A high-level overview of the capabilities of the vSphere key providers requires your attention to help plan your encryption strategy. [Read more]

How vSphere Virtual Machine Encryption Protects Your Environment

Regardless of which key provider you use, with vSphere Virtual Machine Encryption you can create encrypted virtual machines and encrypt existing virtual machines. Because all virtual machine files with sensitive information are encrypted, the virtual machine is protected. Only administrators with encryption privileges can perform encryption and decryption tasks. [Read more]

vSphere Virtual Machine Encryption Components

Depending on which key provider you use, an external key server, the vCenter Server system, and your ESXi hosts are potentially contributing to the encryption solution. [Read more]

Encryption Process Flow

After you set up a key provider, users with the required privileges can create encrypted virtual machines and disks. Those users can also encrypt existing virtual machines and decrypt encrypted virtual machines, and add Virtual Trusted Platform Modules (vTPMs) to virtual machin

cannot add an encrypted disk to a virtual machine that is not encrypted, and you cannot encrypt a disk if the virtual machine is not encrypted. [Read more]

Virtual Machine Encryption Errors

If vCenter Server detects a critical error with virtual machine encryption, it creates an event. You can view these events to help troubleshoot and resolve encryption errors. [Read more]

Prerequisites and Required Privileges for Encryption Tasks

Encryption tasks are possibly only in environments that include vCenter Server. In addition, the ESXi host must have encryption mode enabled for most encryption tasks. The user who performs the task must have the appropriate privileges. A set of **Cryptographic Operations** privileges allows fine-grained control. If virtual machine encryption tasks require a change to the host encryption mode, additional privileges are required. [Read more]

Encrypted vSphere vMotion

vSphere vMotion always uses encryption when migrating encrypted virtual machines. For virtual machines that are not encrypted, you can select one of the encrypted vSphere vMotion options. [Read more]

Encryption Best Practices, Caveats, and Interoperability

Any best practices and caveats that apply to the encryption of physical machines apply to virtual machine encryption as well. The virtual machine encryption architecture results in some additional recommendations. As you are planning your virtual machine encryption strategy, consider interoperability limitations. [Read more]

Key Persistence Overview

In vSphere 7.0 Update 2 and later, encrypted virtual machines and virtual TPMs can continue to optionally function even when the key server is temporarily offline or unavailable. The ESXi hosts can persist the encryption keys to continue encryption and vTPM operations. [Read more]

« Previous Page Next Page »

Support

VMware Customer Connect

Support Policies

Product Documentation

Compatibility Guide

Terms & Conditions

California Transparency Act Statement

Twitter

YouTube

Facebook

LinkedIn

Contact Sales

Terms of Use

Your California Privacy Rights

Privacy

Accessibility

Trademarks

Glossary

Help

Feedback