Protect data at rest with negligible impact on NVMe disk performance metrics

by enabling Secure Enterprise Key Manager on Dell PowerEdge servers

A key advantage to Dell™ Secure Enterprise Key Manager (SEKM) hardware-based encryption is that it protects the data stored on drives in PowerEdge™ servers against multiple threat vectors, including physical removal. You can also use it in conjunction with software-based encryption.

LKM, iLKM, and SEKM

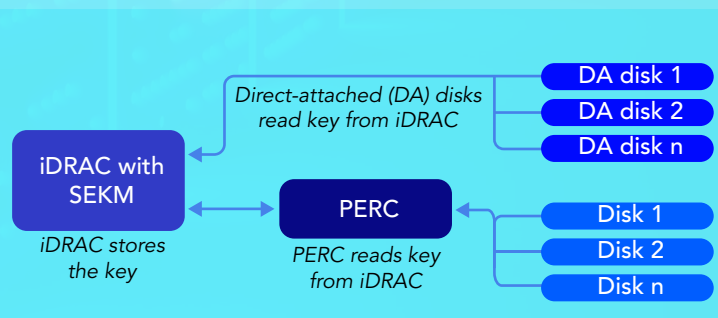
Encryption keys are often targeted by cybercriminals, which makes the proper management of those keys a primary concern for organizations.[1] SEKM, by storing the keys away from the local storage, is the most robust of the three solutions.

Local key management (LKM)

- Standard PERC feature
- No additional licensing or hardware
- Stores the key in the PERC RAID Controller
- Uses pass-phrases to manage access

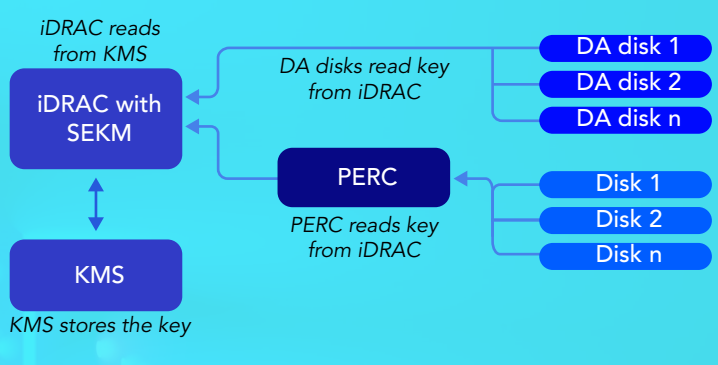
Integrated LKM (iLKM)

- Stores the key in the iDRAC
- Enables key exchange locally
- Requires SEKM license



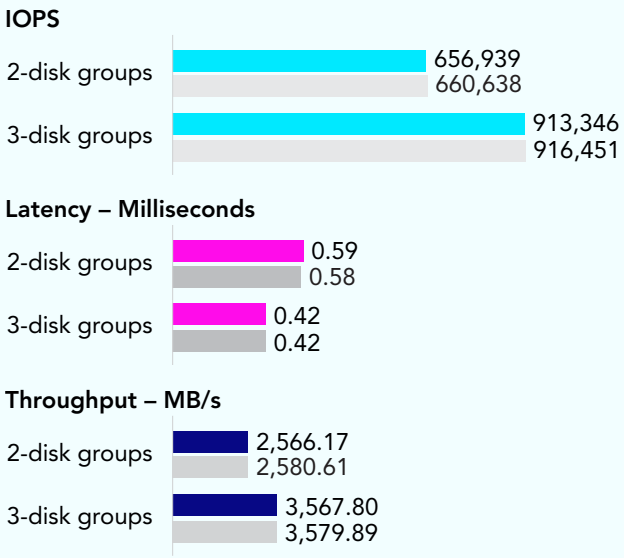
SEKM

- KMIP compliant iDRAC element
- Centralized key management
- Data at rest is inaccessible in compromised drives
- Requires SEKM license and a Key Management Server (KMS)

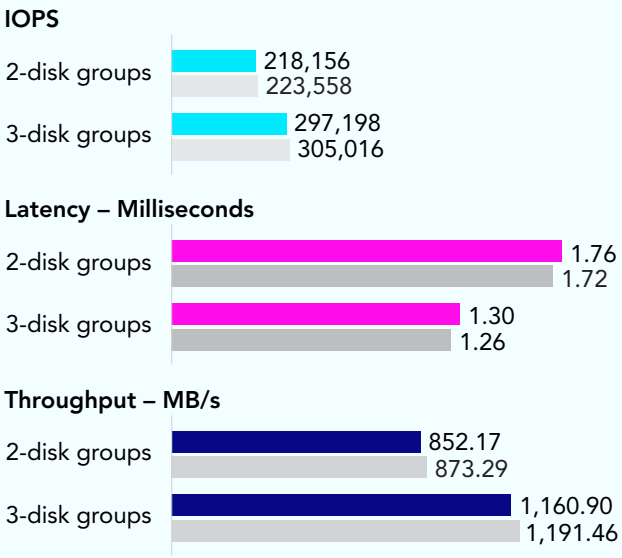


While disk encryption and effective key management are cornerstones to any comprehensive data protection strategy, some IT admins may assume that server storage performance is an associated casualty. In a hyper-converged infrastructure (HCI) cluster containing three Dell PowerEdge R7525 servers in 2- and 3- NVMe® disk group configurations, we found that enabling the SEKM feature had a minimal performance impact on baseline IOPS, latency, and throughput. Additionally, HCI cluster performance scaled linearly when we added storage.

Read tests



Read/write tests



Dell PowerEdge server cluster with SEKM enabled
Dell PowerEdge server cluster without SEKM

Real-world benefits of SEKM security*

Simultaneously secure NVMe and SAS SED drives. — We used the IDRAC to manage both direct-attached NVMe and PERC-attached SAS SEDs.

We switched from iDRAC LKM to SEKM in under 3 minutes. — **Seamlessly change security types.**

Quickly enable SEKM direct-attached encryption. — We configured SEKM direct-attach encryption in under 2.5 minutes.

We enabled firmware updates with no downtime. — **Rebootlessly update drive firmware through the iDRAC.**

**These real-world benefits reflect our hands-on evaluation of the SEKM feature on a Dell PowerEdge R750xs server.*

Learn more at https://facts.pt/jGg1rsF

1 Techopedia, "10 Best Practices for Encryption Key Management," accessed October 19, 2022, https://www.techopedia.com/2/30767/security/10-best-practices-for-encryption-key-management-and-data-security.

Principled Technologies®