

Self-Encrypting Drives in Dell EMC PowerEdge servers with VMware vSphere

Abstract

This technical white paper introduces the Self Encrypting Drives (SED) offered by Dell EMC that helps in encrypting user data by using an encryption circuit built into the storage device controller. This paper describes the configurations required to enable this security feature on SED drives. The use cases demonstrated are for the VMware vSphere and vSAN environments.

June 2020

Revisions

Date	Description
June 2020	Initial release

Acknowledgements

Authors: Rakesh Senapati

Support: Krishnaprasad K, Gurupreet Kaushik

The information in this publication is provided “as is.” Dell Inc. makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any software described in this publication requires an applicable software license.

Copyright © <06/15/2020> Dell Inc. or its subsidiaries. All Rights Reserved. Dell Technologies, Dell, EMC, Dell EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners.

Table of contents

Revisions.....	2
Acknowledgements.....	2
Table of contents	3
Executive summary.....	4
1 Introduction.....	5
1.1 Audience and Scope	5
1.2 Self-Encrypting Drives (SED) support on VMware.....	5
1.3 Hardware and software requirements	5
1.3.1 Prerequisites.....	5
1.3.2 Hardware requirements.....	6
1.3.3 Software requirements	6
2 UEFI or Human Interface Infrastructure (HII) RAID configuration utility	7
3 PERC Command Line Interface (CLI) on VMware ESXi	8
3.1 Monitoring the secure virtual disks within VMware ESXi using PERCCLI	8
4 iDRAC Storage Configuration	14
5 Dell OpenManage Server Administrator	15
5.1 Configure Dell OMSA on VMware ESXi.....	15
5.2 Configure Dell OMSA on Windows operating system.....	15
6 vSAN with Self Encrypting Drive (SED)	16
7 Summary	17
8 References	18

Executive summary

Self-Encrypting Drives (SED) comply with the Opal Storage Specification, created by TCG Storage Security Subsystem. It is a set of security specifications for features of data storage devices such as disk drives that enhance their security. This document is intended to help the user build a configuration with encrypted virtual disks to get data-at-rest protection and use the same from a VMware vSphere point of view. For information on OPAL and TCG, see <https://trustedcomputinggroup.org/>.

1 Introduction

The Self-Encrypting Drives (SED) are hard disks or solid-state drives that integrate encryption of user data at rest. SED perform encryption or decryption in real-time and these operations are entirely transparent to the user.

The encryption and decryption are performed using a Media Encryption Key (MEK), also known as Data Encryption Key (DEK) generated internally in the storage device. SED hardware handles this encryption in real-time with no impact on performance. The MEK is not revealed anywhere externally on the drive.

SED provides two important features:

- Protect the user data from unauthorized access by auto-locking in the event of the drive being misplaced or stolen from a system while in use (secure DAR).
- Cryptographic Erase or secure erase feature. This is a mechanism to securely erase the data on the drive so that the drive can be repurposed or retired.

1.1 Audience and Scope

The intended audience for this whitepaper includes system administrators who are familiar with data center operations. This white paper is mainly intended for users who wants to understand Self Encrypting Drives significance from VMware vSphere perspective.

1.2 Self-Encrypting Drives (SED) support on VMware

Dell EMC supports SED drives for VMware vSphere however, support for vSAN is not provided. SED drives can be used for vSAN by disabling encryption at the Hardware level if the same is listed in the vSAN HCL Database. For more information on vSAN encryption, see [vSAN Frequently Asked Questions \(FAQ\)](#).

1.3 Hardware and software requirements

Dell PowerEdge RAID Controller (PERC) cards support Self-Encrypting Disks (SED) for protection of data against loss or theft of SEDs. A security key known as KEK is assigned for each controller. The security key can be managed under Local Key Management (LKM).

This security key is used by the controller to unlock the drive so that the drive can use the Data Encryption Key (DEK). The hashed Key Encryption Key (KEK) is stored on the PERC controller and never exposed outside to controller.

1.3.1 Prerequisites

The following are the prerequisites for utilizing SED drives on Dell EMC PowerEdge server:

- PERC controllers with RAID qualified for encryption.
- SED Drives
- Security Key
- Virtual disk with Security feature enabled.

All Self-Encrypting Disks are qualified for encryption however, the user needs to create virtual disks with physical SED drives to secure the data.

1.3.2 Hardware requirements

Dell EMC offers SEDs only on PERC h7xx, h8x0, and PERC fd33xd controllers. The PERC h3xx (PERC H345, PERC H330 and PERC H310) series cards are not supported by Encryption Key Management features however, the SED drives can be used as standard hard drives.

Managing the encryption key task is not supported on PERC hardware controllers running in HBA mode. SAS HBA controller does not support SED drives however, the SED drives can be used as standard hard drives.

The table below lists the PERC cards which are LKM Supported for enabling Encryption Key.

Table 1 Managing the Encryption Key Task Supported PERC Hardware Controllers

PERC Series	Related PERC	Manage Encryption Key Task Supported
PERC 10	PERC H745 Front card & Adapter	Yes
	PERC H740P	Yes
	PERC H840	Yes
	PERC H745P MX	Yes
PERC 9	PERC H730	Yes
	PERC H730P	Yes
	PERC H730P MX	Yes
	PERC H830	Yes
	PERC FD33xD/ PERC FD33xS	Yes
	Shared PERC	Yes
PERC 8	PERC H710	Yes
	PERC H710P	Yes
	PERC H810	Yes

1.3.3 Software requirements

Encryption or decryption operations are completely transparent to VMware ESXi and cannot be identified, monitored or managed from the vCenter Server or the host and the client without third party utilities such as, PowerEdge RAID Controller (PERC) Command Line Interface (CLI). Listed below are the different ways in which Security key and Security on Virtual Disks can be managed and enabled:

- UEFI or Human Interface Infrastructure (HII) RAID configuration utility
- PowerEdge RAID Controller Command Line Interface (PERCCLI) utility
- iDRAC Storage Configuration
- OpenManage Server Administrator (OMSA)

2 UEFI or Human Interface Infrastructure (HII) RAID configuration utility

Note: A SED drive connected to PERC H745P MX storage controller placed in a Dell EMC PowerEdge MX840c server is used in this section to configure it as an Encrypted Virtual Disk.

Follow the steps below:

1. Check the drive encryption capability by choosing **Storage Dashboard > Physical Disk Management > Advanced**.
2. Once the SED drive is configured as an Encrypted Virtual Disk, the value of **Secured** is set to **Yes** if the device is configured. This value is **No** if the device is not configured.
3. To enable Local Key Management (LKM) on the controller and to create Secure Virtual Disk with SED drives follow the user guide [Security Key and RAID Management](#).
4. For the respective PERC adapter documentation, see the [Storage Adapter and Controllers](#) page and select the specific storage controller. Select the **Documentation** tab and click on the **Manuals and Documents** section from the left pane.

3 PERC Command Line Interface (CLI) on VMware ESXi

Command line interfaces and GUIs are not available on VMware ESXi to monitor the usage of the SED drive. However, there are vendor utilities such as, PERCCLI that provide this feature.

Follow the steps below to install PERCCLI on VMware ESXi:

1. Download the PERCCLI utility compatible for VMware ESXi from www.dell.com/support. The percli.gz file can be downloaded by using the keyword PERCCLI.

Note: Before downloading the percli.gz file, click on **View full driver details** and check the **Fixes and Enhancements** section to match the HBA/PERC card support.

2. Extract the PERCcli_VMWare_XXXXX_xxx_x.XXX.tar.gz file to /vmfs/volume/datastore1 on the host using the following command:

```
tar -xvf PERCcli_VMWare_XXXXX_xxx_x.XXX.tar.gz
```

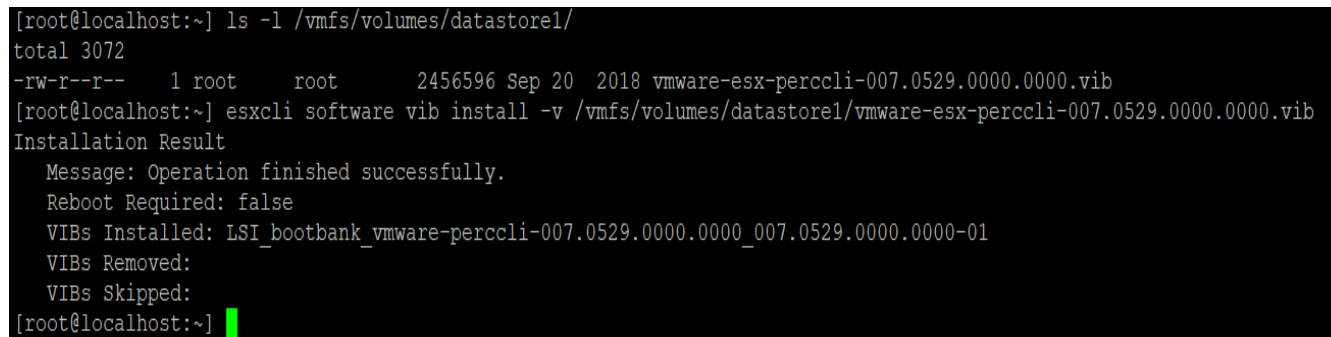
3. View the list of installed VIB packages using the following command:

```
esxcli software vib list
```

4. Install the VIB package using the command:

```
esxcli software vib install -v /vmfs/volume/datastore1/vmware-perccli-xxx.xxxx.xxxx.xxxx.vib
```

Here, /vmfs/volume/datastore1 is the path of the stored VIB.



```
[root@localhost:~] ls -l /vmfs/volumes/datastore1/
total 3072
-rw-r--r-- 1 root root 2456596 Sep 20 2018 vmware-esx-perccli-007.0529.0000.0000.vib
[root@localhost:~] esxcli software vib install -v /vmfs/volumes/datastore1/vmware-esx-perccli-007.0529.0000.0000.vib
Installation Result
Message: Operation finished successfully.
Reboot Required: false
VIBs Installed: LSI_bootbank_vmware-perccli-007.0529.0000.0000_007.0529.0000.0000-01
VIBs Removed:
VIBs Skipped:
[root@localhost:~] █
```

Figure 1 PERCCLI utility installed on VMware ESXi

3.1 Monitoring the secure virtual disks within VMware ESXi using PERCCLI

Screenshots used in this section are captured from VMware ESXi 6.7 with the following configurations:

- ESXi 6.7 U3 Dell Version: A04, Build# 15160138
- PERCCLI Utility version - 7.529.00 (A07)
- Server PowerEdge R6515
- Storage Card H740P Mini
- System installed with BIOS firmware 1.2.14

- PERC Storage Card Firmware 50.9.4-3025
- SED Drive Model- SEAGATE (ST2400MM0149)

Listed below are command lines offered in the PERCCLI package that can be used to monitor SED drives within VMware ESXi:

1. Run PERCCLI by browsing to the following location:

```
cd /opt/lsi/perccli
```

2. The following PERCCLI utility screenshot displays information about Encryption Capable Drive and SED enabled Virtual Disk using the command:

```
./perccli /c0 show all
```

```

Drive Groups = 2

TOPOLOGY :
=====

-----
DG Arr Row EID:Slot DID Type State BT Size PDC PI SED DS3 FSpace TR
-----
0 - - - - RAID0 Optl N 1.090 TB dflt N N dflt N N
0 0 - - - RAID0 Optl N 1.090 TB dflt N N dflt N N
0 0 0 64:1 1 DRIVE Onln N 1.090 TB dflt N N dflt - N
1 - - - - RAID0 Optl N 2.182 TB dflt N Y dflt N N
1 0 - - - RAID0 Optl N 2.182 TB dflt N Y dflt N N
1 0 0 64:2 2 DRIVE Onln N 2.182 TB dflt N Y dflt - N
-----

DG=Disk Group Index|Arr=Array Index|Row=Row Index|EID=Enclosure Device ID
DID=Device ID|Type=Drive Type|Onln=Online|Rbld=Rebuild|Dgrd=Degraded
Pgdg=Partially degraded|Offln=Offline|BT=Background Task Active
PDC=PD Cache|PI=Protection Info|SED=Self Encrypting Drive|Frqn=Foreign
DS3=Dimmer Switch 3|dflt=Default|Msng=Missing|FSpace=Free Space Present
TR=Transport Ready

Virtual Drives = 2

VD LIST :
=====

-----
DG/VD TYPE State Access Consist Cache Cac sCC Size Name
-----
0/0 RAID0 Optl RW Yes RWBD - OFF 1.090 TB raid0
1/1 RAID0 Optl RW Yes RWBD - OFF 2.182 TB Virtual Disk1
-----

Cac=CacheCade|Rec=Recovery|OfLn=OffLine|Pgdg=Partially Degraded|Dgrd=Degraded
Optl=Optimal|RO=Read Only|RW=Read Write|HD=Hidden|TRANS=TransportReady|B=Blocked|
Consist=Consistent|R=Read Ahead Always|NR=No Read Ahead|WB=WriteBack|
FWB=Force WriteBack|WT=WriteThrough|C=Cached IO|D=Direct IO|sCC=Scheduled
Check Consistency

Physical Drives = 2

PD LIST :
=====

-----
EID:SlT DID State DG Size Intf Med SED PI SeSz Model Sp Type
-----
64:1 1 Onln 0 1.090 TB SAS HDD N N 512B ST1200MM0088 U -
64:2 2 Onln 1 2.182 TB SAS HDD Y N 512B ST2400MM0149 U -
-----

```

Figure 2 Information on Encryption Capable Drive and SED enabled Virtual Disk

- Following screenshot shows that the controller has configured with Local Key Manager making use of the following command:

```
./perccli /c0 show all
```

```
Status :
=====
Controller Status = Optimal
Memory Correctable Errors = 0
Memory Uncorrectable Errors = 0
ECC Bucket Count = 0
Any Offline VD Cache Preserved = No
BBU Status = 0
PD Firmware Download in progress = No
Lock Key Assigned = Yes
Failed to get lock key on bootup = No
Lock key has not been backed up = No
Bios was not detected during boot = No
Controller must be rebooted to complete security operation = No
A rollback operation is in progress = No
At least one PFK exists in NVRAM = No
SSC Policy is WB = No
Controller has booted into safe mode = No
Current Personality = RAID-Mode
```

Figure 3 Controller has been configured with Local Key Manager

- To create a RAID volume using SED drive for a non-secured VD, use the following command:

```
./perccli /c0 add vd r0 drives=64:2
```

```
[root@localhost:/opt/lsi/perccli] ./perccli /c0 add vd r0 drives=64:2
CLI Version = 007.0529.0000.0000 Sep 18, 2018
Operating system = VMkernel 6.7.0
Controller = 0
Status = Success
Description = Add VD Succeeded
```

Figure 4 RAID volume using SED drive for a non-secured VD created

- To encrypt the non-secured virtual disk using the following command:

```
./perccli /c0/d1 set security=on
```

Here, d1 stands for DiskGroup 1.

Note: Physical drive should have the SED capable feature

```
[root@localhost:/opt/lsi/perccli] ./perccli /c0/d1 set security=on
CLI Version = 007.0529.0000.0000 Sep 18, 2018
Operating system = VMkernel 6.7.0
Controller = 0
Status = Success
Description = Success
```

Figure 5 Non-secure virtual disk encrypted

- To create a RAID volume directly with SED capable drive, use the following command:

```
./perccli /c0 add vd r0 drives=64:2 sed
```

Here, RAID type is RAID-0, Enclosure ID 64, Drive Slot ID 2 and sed option for creating security-enabled drive.

```
[root@localhost:/opt/lsi/perccli] ./perccli /c0 add vd r0 drives=64:2 sed
CLI Version = 007.0529.0000.0000 Sep 18, 2018
Operating system = VMkernel 6.7.0
Controller = 0
Status = Success
Description = Add VD Succeeded
```

Figure 6 RAID volume created directly with SED capable drive

- To erase data and security information on the SED Physical Drive, use the following command:

```
./perccli /c0/e64/s2 secureerase force
```

Here, Enclosure ID is 64 and the drive Slot ID is 2.

Note: In order to perform this erase, the physical drive must be in an unconfigured state.

```
[root@localhost:/opt/lsi/perccli] ./perccli /c0/e64/s2 secureerase force
CLI Version = 007.0529.0000.0000 Sep 18, 2018
Operating system = VMkernel 6.7.0
Controller = 0
Status = Success
Description = Drive Secure Erase Succeeded.
```

Figure 7 Data and security information erased on the SED Physical Drive

- To display information about the physical drive, including device attribute, settings, and port information for a specific slot in the controller, use the command:

```
./perccli /c0/e64/s2 show all
```

Here, Enclosure ID is 64 and the Drive Slot ID is 2.

Note: If the **SED Enabled and Secured** option is displayed as **No**, then the SED capable drive is not configured with encryption.

```

Drive /c0/e64/s2 Policies/Settings :
=====
Drive position = DriveGroup:1, Span:0, Row:0
Enclosure position = 1
Connected Port Number = 0(path0)
Sequence Number = 2
Commissioned Spare = No
Emergency Spare = No
Last Predictive Failure Event Sequence Number = 0
Successful diagnostics completion on = N/A
SED Capable = Yes
SED Enabled = Yes
Secured = Yes
Cryptographic Erase Capable = Yes
Locked = No
Needs EKM Attention = No
PI Eligible = No
Certified = Yes
Wide Port Capable = No

```

Figure 8 Display drive details

9. Check the mapped virtual disk information on VMware ESXi OS using the following command:

```
esxcli storage core device list
```

10. To create multiple RAID 0 virtual disks with each SED drive connected to the drive backplane, use the following command:

```
./perccli /c0 add vd each r0 sed
```

For more PERCCLI commands, see [Dell EMC PowerEdge RAID Controller CLI Reference Guide](#).

4 iDRAC Storage Configuration

The Integrated Dell Remote Access Controller (iDRAC) embedded in Dell EMC PowerEdge servers allows you to deploy, update, monitor and maintain PowerEdge servers with or without a systems management software agent. iDRAC also helps to manage storage related functions on the system at run-time. You can perform virtual disk encryption with SED drives through iDRAC. Though encryption is enabled in the controllers, encryption must be manually enabled on the virtual disk, if it is created using iDRAC.

Note: The following section demonstrates how to enable encryption on a virtual disk created through iDRAC GUI with SED drives.

Follow the steps below to encrypt the virtual disk:

1. In the iDRAC web interface, go to **Configuration > Storage Configuration**.
2. From the **Controller drop-down menu**, select the controller to view the created virtual disks.
3. Click **Virtual Disk Configuration**. All the virtual disks associated to the controller are displayed.
4. To enable security in the virtual disk, from the **Action** pane, select **Encrypt Virtual Disks**.
5. Click **Apply Now**. Depending on your requirement, you can also choose to apply **At Next Reboot** or **At Scheduled Time**. Based on the selected operation mode, the settings are applied.

For more information about iDRAC storage configuration, see [Remote Enterprise Systems Management](#).

5 Dell OpenManage Server Administrator

Dell OpenManage Server Administrator (OMSA) is a complementary tool that provides a comprehensive, one-to-one systems management solution. OMSA provides this solution in two ways:

- An integrated, web browser-based graphical user interface (GUI)
- Command Line Interface (CLI) through the operating system.

OMSA can be used to manage Local Key Manager (LKM) on storage controllers which helps in encrypting the virtual disk.

5.1 Configure Dell OMSA on VMware ESXi

To download and install Dell OpenManage Server Administrator VIB according to your VMware ESXi version and the server model, follow the steps below:

1. Go to www.dell.com/support and enter the system service tag or the server model number.
2. Select on the Drivers and Downloads tab and choose the corresponding operating system.
3. Search for the vib package using the keyword OMSA.
4. Extract the OM-SrvAdmin-Dell-Web-x.x.x-xxxx.VIB-ESX67i_A00 zip file.
5. Upload the VIB to the Datastore using winscp or vSphere web client.
6. Install the VIB package using the following command:

```
esxcli software vib install -v
/vmfs/volume/datastore1/Dell_bootbank_OpenManage_x.x.x.ESXixxx-xxxx.vib
```

5.2 Configure Dell OMSA on Windows operating system

To download and install Dell OpenManage Server Administrator on Windows OS, follow the steps below:

1. To access the OMSA installed on ESXi host remotely, download and install OMSA application on the management or client system running Windows operating system.
2. Download the Dell OMSA application for Windows operating system from www.dell.com/support or see [Support for Dell EMC OpenManage Server Administrator \(OMSA\)](#).
3. Once the OMSA zip file is downloaded, install the setup.exe from the folder path: C:\OpenManage\windows. After the installation, open Dell OpenManage Server Administrator from the desktop shortcut created.
4. Manage the OMSA interface by providing the IP address of the ESXi host in **Server Administrator** launcher, user (root) and password.
5. Select the checkbox for the option **Ignore certificate warnings**.

For more information on how to manage LKM and encrypt the virtual disk, see [OpenManage Server Administrator Storage Management User guide\(s\)](#).

6 vSAN with Self Encrypting Drive (SED)

vSAN is a software defined storage which provides a software-based encryption to support data at rest encryption on any storage device. vSAN is also FIPS compliant and hence, there is no requirement for an SED drive which can be 15 to 30 percent more expensive than a standard drive. SED drives can still be used for vSAN by disabling the SED functionality in the hardware.

7 Summary

This white paper introduces the Self Encrypting Drives (SED) feature offered by Dell EMC to administrators and users for enabling encryption to achieve data-at-rest protection and use the same from a VMware vSphere environment. This paper also describes how PERCCLI can be installed on VMware ESXi allowing us to monitor the secure virtual disks within VMware ESXi. iDRAC and OMSA configurations have also been described to help users manage LKM and encrypt virtual disks.

8 References

- [VMware vSphere Virtual Machine Encryption Management](#)
- [vSAN Frequently Asked Questions \(FAQ\)](#)
- [Trusted Computing Group](#)
- [Trusted Computing Group and NVM Express Joint White Paper: TCG Storage, Opal, and NVMe](#)
- [NIST Guidelines for Media Sanitization](#)