UEFI Secure Boot with Dell PowerEdge 14G with VMware ESXi 6.5

This paper explains the changes introduced in UEFI Secure Boot feature from DellEMC 14th generation of servers and VMware ESXi upgrade scenarios.

Dell OS and Hypervisor Engineering
July 2017

Authors

Bill Munger

Gobind Vijayakumar

Thiru Navukkarasu

Krishnaprasad K

A Dell EMC Technical White Paper

Revisions

Date	Description
July 2017	Initial release

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.

Dell believes the information in this document is accurate as of its publication date. The information is subject to change without notice.

Table of Contents

Introduction

Dell EMC PowerEdge 14G Servers is the next generation of servers in Dell EMC Servers portfolio and it comes with a lot of innovative features. In this blog, we are going to discuss more on the UEFI Secure Boot Feature in our 14G Servers and its support with VMware ESXi 6.5.

UEFI Secure Boot first appeared in the UEFI 2.3.1 specification, and the Dell server BIOS included support beginning with 13th generation servers. With 14G Servers one of the updates is the addition of two new Secure Boot modes named Deployed Mode and Audit Mode. These two modes add to the original modes Setup Mode and User Mode to provide the user with a total of four modes. Refer to this Dell whitepaper for further background on the UEFI Secure Boot feature.

Note: UEFI SecureBoot relies on four key variables present in the UEFI BIOS namely PK, KEK, DB and DBX.

Platform Key (PK): An X.509 certificate containing a public key used to verify any updates to the Key Exchange Key (KEK) database or any updates to PK itself. PK must be present before Secure Boot can be enabled.

Key Exchange Key (KEK): One or more X.509 certificates used to verify any updates to the signature databases (db and dbx)

db: The Authorized Signature Database is used to authorize signed efi binaries and loadable roms when Secure Boot is enabled.

dbx: The Forbidden signatures database is used to detect unauthorized efi binaries and loadable roms when Secure Boot is enabled.

UEFI Secure Boot modes with Dell PowerEdge 14G Servers

UEFI Secure Boot BIOS setting enables Secure Boot, where the BIOS authenticates each pre-boot image by using the certificates in the Secure Boot Policy. Secure Boot is disabled by default. When Secure Boot Policy is set to Standard, the BIOS uses the system manufacturer's key and certificates to authenticate pre-boot images. When Secure Boot policy is set to Custom, the BIOS uses the user-defined key and certificates. Secure Boot policy is set to Standard by default.

Secure Boot Policy Summary specifies the list of certificates and hashes that Secure Boot uses to authenticate images.

Setup Mode - In Setup Mode, the BIOS performs no signature verification on updates to Secure Boot policy objects (PK, KEK, db, dbx). Any software can update policy objects in Setup Mode.

User Mode – User Mode means that someone has installed a Platform Key (PK), but has not yet deployed the system (i.e. has not yet made the system available for everyday use). In UEFI 2.3.1, User Mode was considered secure because BIOS performed signature verification on any updates to Secure Boot policy objects. However, with the introduction of Audit Mode in UEFI 2.5 and later, User Mode is no longer considered secure. This is because, while the system is in User Mode, any software may set the Audit Mode variable, causing the BIOS to remove PK and to stop verifying updates to Secure Boot policy objects.

Audit Mode - Audit Mode (new in UEFI 2.5) helps the user discover the effects of changes to Secure Boot policy objects. In this mode, the BIOS performs signature verification on pre-boot code modules as if the system were in User Mode with Secure Boot enabled, but allows all modules to load whether they pass verification or not. The BIOS records the results of signature verification in the Image Execution Information Table (IEIT) as explained in UEFI spec v2.6, section 30.4.2.

- *Important Note:*
  - *This mode is supported in BIOS, but not yet supported by Operating System Vendors. Dell strongly recommends using Deployed Mode for normal system operations.*
  - *By Default, Only user mode and Deployed mode are available in System BIOS. Configuration changes in BIOS Setup are required before Audit Mode is available. Advanced users who want to more about transitioning to Audit Mode can refer to Figure 77 in the UEFI 2.6 spec (or Figure 83 in UEFI 2.7 spec).*

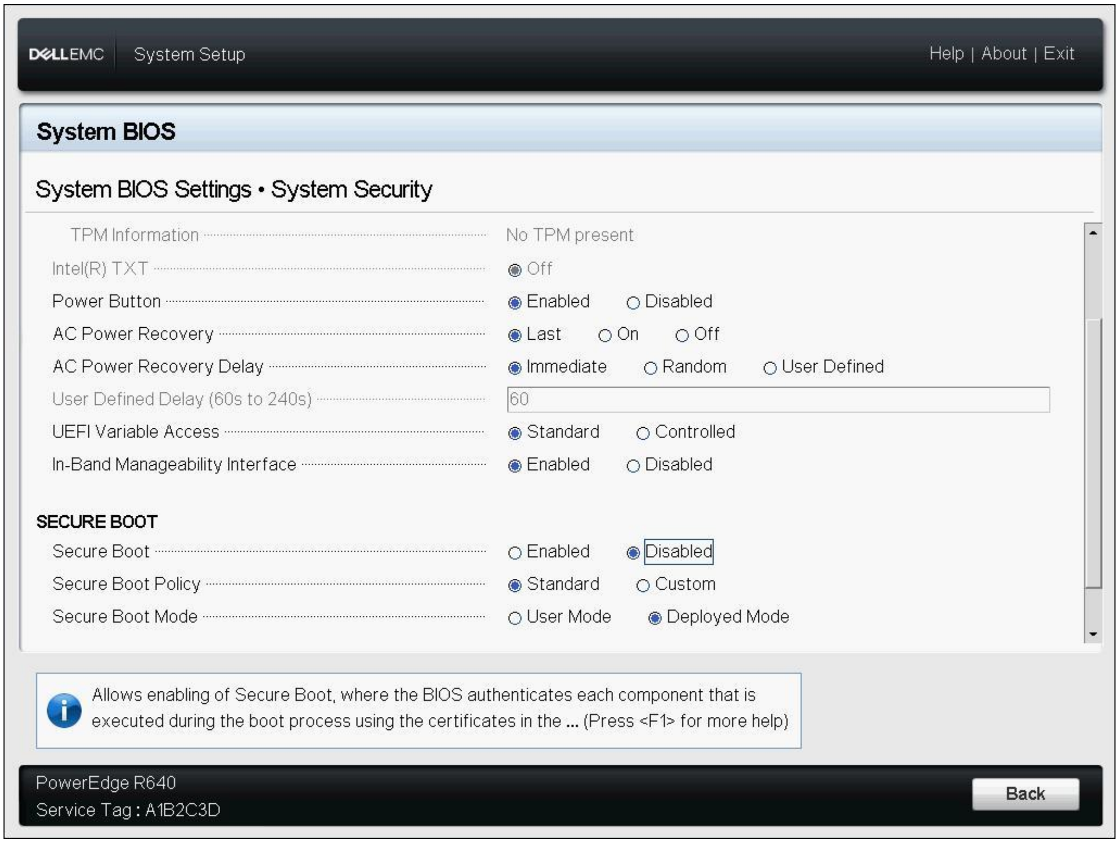
Deployed Mode – Deployed Mode is the most secure mode, intended for everyday secure operation of the system. Users use Setup, Audit, and User Mode to provision or configure a system, then transition to Deployed Mode before making the system available for general use.

[Reference – UEFI 2.6 Spec]

Installing VMware ESXi on Dell PowerEdge 14G Server with Secure Boot Enabled

Note: ESXi versions above VMware ESXi 6.5 supports UEFI Secure Boot. Refer to VMWare documentation on UEFI Secure Boot.

1) Go into System BIOS -> System Security and Toggle Secure Boot to Enabled.



System BIOS

System BIOS Settings • System Security

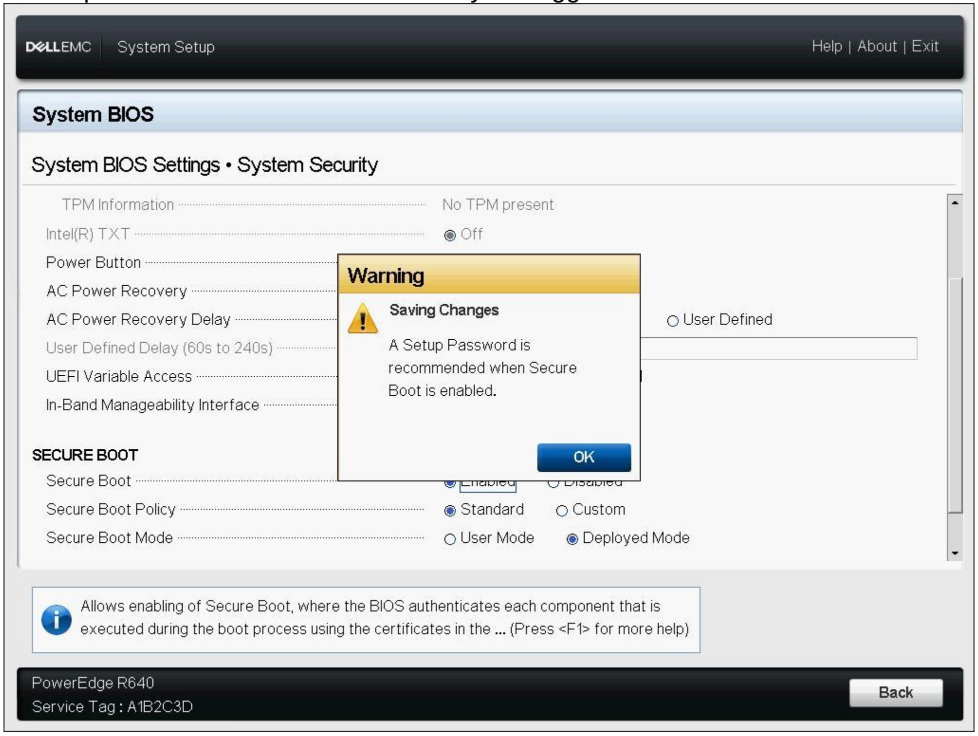
TPM Information .... No TPM present
Intel(R) TXT .... ● Off
Power Button .... ● Enabled ○ Disabled
AC Power Recovery .... ● Last ○ On ○ Off
AC Power Recovery Delay .... ● Immediate ○ Random ○ User Defined
User Defined Delay (60s to 240s) 60
UEFI Variable Access .... ● Standard ○ Controlled
In-Band Manageability Interface .... ● Enabled ○ Disabled

SECURE BOOT
Secure Boot .... ○ Enabled ● Disabled
Secure Boot Policy .... ● Standard ○ Custom
Secure Boot Mode .... ○ User Mode ● Deployed Mode

Allows enabling of Secure Boot, where the BIOS authenticates each component that is executed during the boot process using the certificates in the ... (Press <F1> for more help)

PowerEdge R640
Service Tag : A1B2C3D

2) A Setup Password is recommend once you Toggle it to Enabled.



DELLEMC System Setup Help | About | Exit

System BIOS

System BIOS Settings • System Security

TPM Information	No TPM present
Intel(R) TXT	● Off
Power Button	
AC Power Recovery	
AC Power Recovery Delay	○ User Defined
User Defined Delay (60s to 240s)	
UEFI Variable Access	
In-Band Manageability Interface	
SECURE BOOT	
Secure Boot	● Enabled ○ Disabled
Secure Boot Policy	● Standard ○ Custom
Secure Boot Mode	○ User Mode ● Deployed Mode

Warning

Saving Changes

A Setup Password is recommended when Secure Boot is enabled.

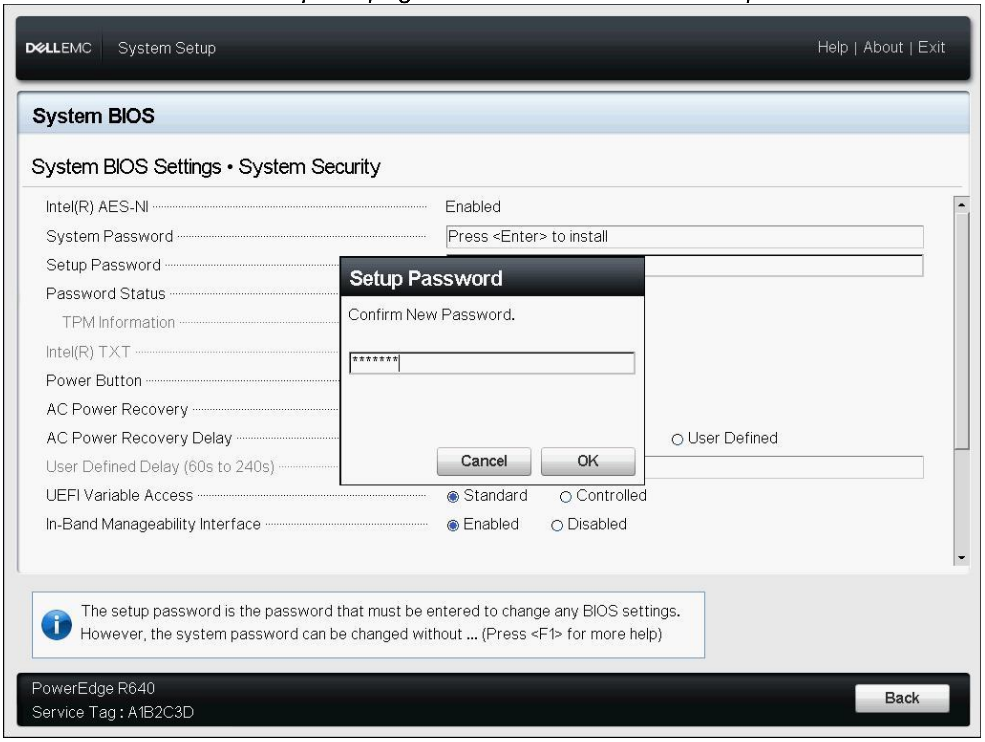
OK

Allows enabling of Secure Boot, where the BIOS authenticates each component that is executed during the boot process using the certificates in the ... (Press <F1> for more help)

PowerEdge R640
Service Tag : A1B2C3D

Back

3) Please provide the setup password and confirm the same as below
Note: We need to scroll up the page in order to locate the 'Setup Password' field



DELLEMC System Setup Help | About | Exit

System BIOS

System BIOS Settings • System Security

Intel(R) AES-NI	Enabled
System Password	Press <Enter> to install
Setup Password	
Password Status	
TPM Information	
Intel(R) TXT	
Power Button	
AC Power Recovery	
AC Power Recovery Delay	○ User Defined
User Defined Delay (60s to 240s)	
UEFI Variable Access	● Standard ○ Controlled
In-Band Manageability Interface	● Enabled ○ Disabled

Setup Password

Confirm New Password.

****

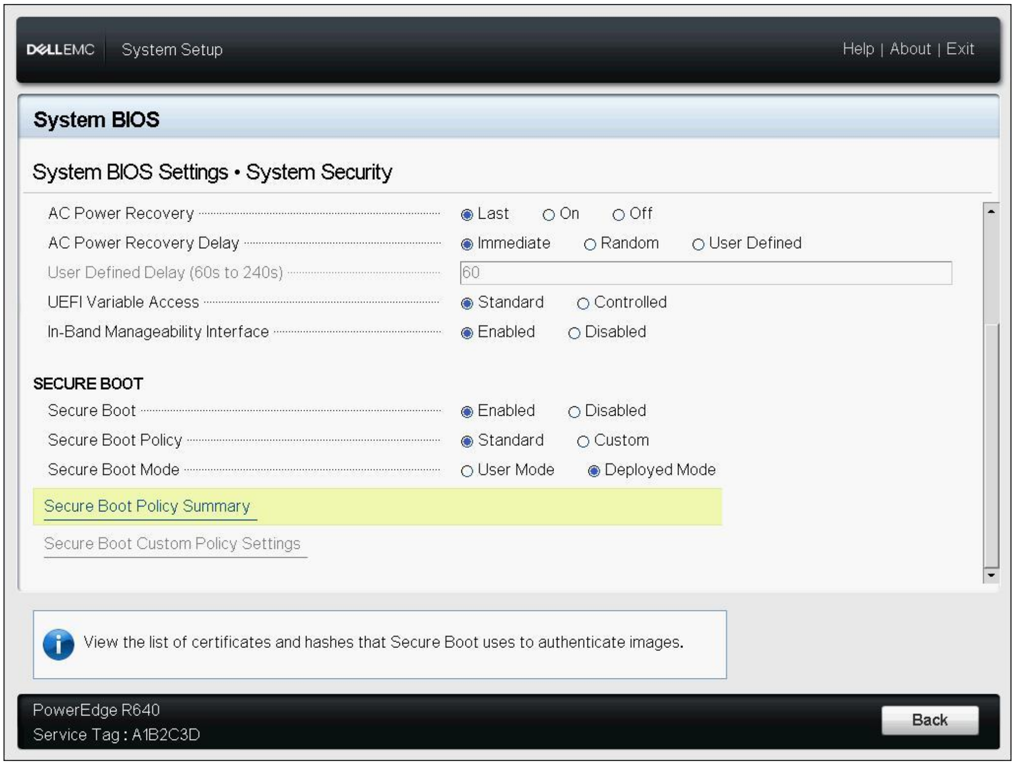
Cancel OK

The setup password is the password that must be entered to change any BIOS settings. However, the system password can be changed without ... (Press <F1> for more help)

PowerEdge R640
Service Tag : A1B2C3D

Back

4) Verify the settings are reflected as below. Save the settings the exit the Menu.



System BIOS

System BIOS Settings • System Security

AC Power Recovery ● Last ○ On ○ Off

AC Power Recovery Delay ● Immediate ○ Random ○ User Defined

User Defined Delay (60s to 240s) 60

UEFI Variable Access ● Standard ○ Controlled

In-Band Manageability Interface ● Enabled ○ Disabled

SECURE BOOT

Secure Boot ● Enabled ○ Disabled

Secure Boot Policy ● Standard ○ Custom

Secure Boot Mode ○ User Mode ● Deployed Mode

Secure Boot Policy Summary

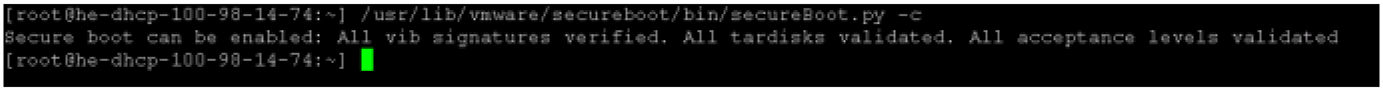
Secure Boot Custom Policy Settings

View the list of certificates and hashes that Secure Boot uses to authenticate images.

PowerEdge R640
Service Tag : A1B2C3D

5) Deploy ESXi Installer using a CD/DVD or Virtual Media

6) Post Install – Run the below script in ESXi Shell and verify if the SecureBoot is enabled

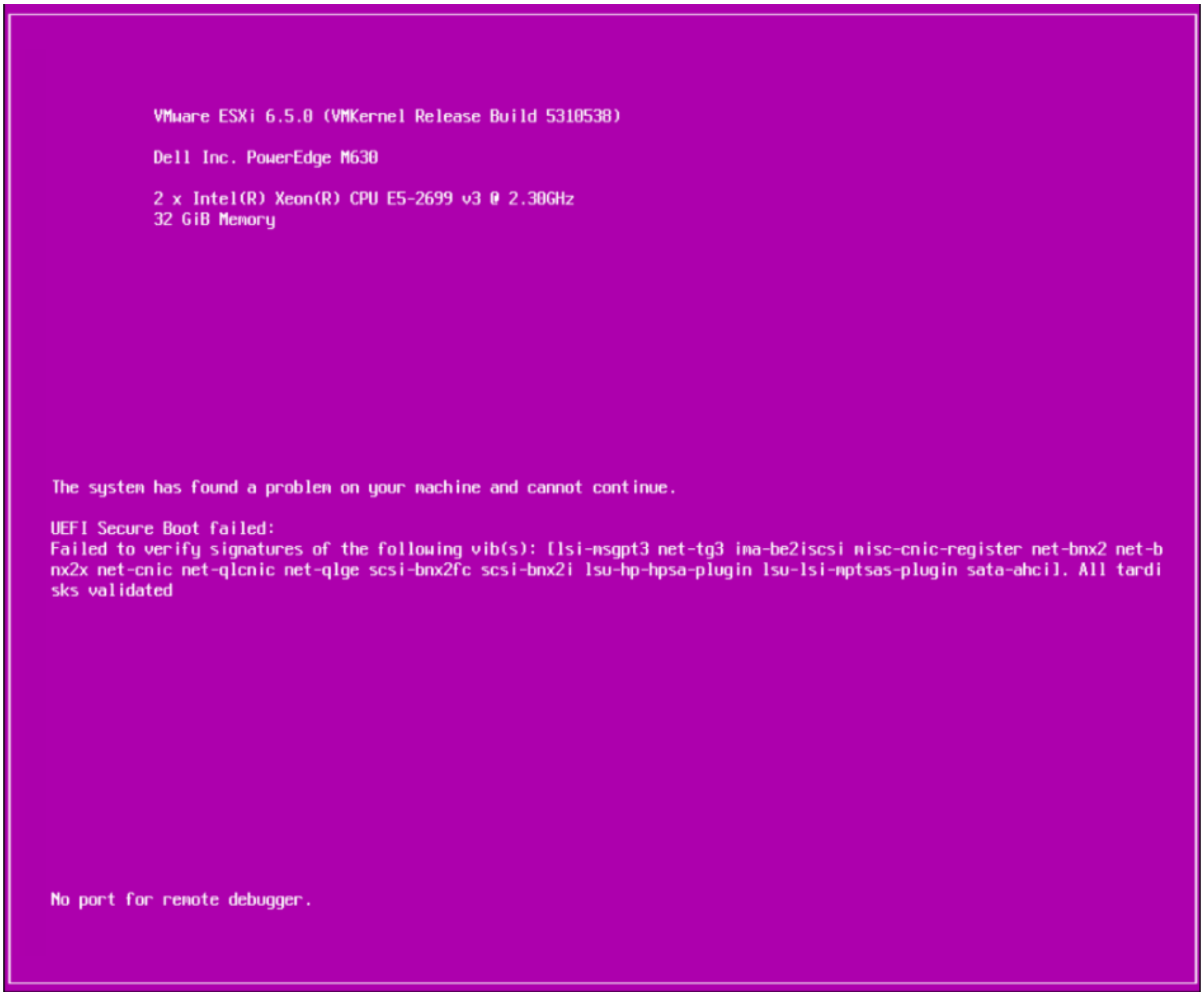


```
[root@he-dhcp-100-98-14-74:~] /usr/lib/vmware/secureboot/bin/secureBoot.py -c
Secure boot can be enabled: All vib signatures verified. All tardisks validated. All acceptance levels validated
[root@he-dhcp-100-98-14-74:~]
```

Limitations with ESXi Upgrade with UEFI Secure Boot

VMware has already documented certain limitations w.r.t UEFI secureboot when ESXi is upgraded from previous versions to 6.5 which does not support Secure Boot support. Refer to VMware KB 2147606

Let’s take a scenario where a user upgrades a system from VMware ESXi 6.0U3 Dell customized image (A03) to 6.5 customized image (A04). Post enabling UEFI Secure Boot in system BIOS, System fails to boot. Below is a sample snapshot of the PSOD during system boot post VMware ESXi upgrade from 6.0 U3 to 6.5 with UEFI Secure Boot enabled. **NOTE** that the package list which shows the signature failure can vary depending upon the versions from which you upgraded.



```
          VMware ESXi 6.5.0 (VMKernel Release Build 5310538)

          Dell Inc. PowerEdge M630

          2 x Intel(R) Xeon(R) CPU E5-2699 v3 @ 2.30GHz
          32 GiB Memory

The system has found a problem on your machine and cannot continue.

UEFI Secure Boot failed:
Failed to verify signatures of the following vib(s): [lsi-msgpt3 net-tg3 ima-be2iscsi misc-cnic-register net-bnx2 net-b
nx2x net-cnic net-qlcnic net-qlge scsi-bnx2fc scsi-bnx2i lsu-hp-hpsa-plugin lsu-lsi-mptsas-plugin sata-ahci]. All tardi
sks validated

No port for remote debugger.
```

NOTE: Dell highly recommends users to run the Secureboot.py script as inferred in the whitepaper before upgrading so that any VIB's which is not required in your system and doesn't carry the required signature can be removed (OR) necessary decisions can be made on enabling secureboot.

Dell Recommends customers to review the VIB's and take decisions as appropriate.

- If the VIB is a boot-critical driver, it's not advised to remove the boot critical VIB. It's recommended to review if VMware ESXi upgrade is mandatory in your production environment. Dell's recommendation is to reinstall VMware ESXi 6.5 if you look for enabling UEFI Secure Boot in this case.
- If it is a non-boot critical driver and the VIB is not utilized, then it can be removed from ESXi using 'esxcli software vib remove –n <VIB ID>'. Refer to VMware KB 2147606.

As an example, below are the list of VIBs which causes Secure Boot to fail when users upgrade from Dell customized 6.0 U3 A03 version to Dell customized VMware ESXi 6.5 A04. This is to emphasize that it's very important to review and understand the VIB signatures which are failing and make a decision to remove the packages from ESXi if at all UEFI Secure Boot needs to be enabled post upgrade.

lsi-msgpt3	This is a storage driver which is used to enable Dell HBA330 as well as 12Gbps storage controllers. This can be a boot critical driver if ESXi is installed on a drive which is exposed via the above mentioned controllers.
net-tg3	This is a network driver used to enable 1Gbps network devices. Removing this VIB can lose the network connectivity based on how you make use of this device in your environment.
ima-be2iscsi	This is a supporting library package for be2iscsi Emulex iSCSI driver.
misc-cnic-register	This is a supporting package used for Broadcom drivers.
net-bnx2	This is a driver package which is used to enable 1Gbps Broadcom network devices. Removing this VIB can may impact the network connectivity based on how you make use of this device in your environment.
net-bnx2x	This is a driver package which is used to enable 10Gbps Broadcom network devices. Removing this VIB may impact the network connectivity based on how you make use of this device in your environment.
net-cnic	This is a supporting package used for Broadcom drivers.
net-qlcnic	This is a driver package used to enable Qlogic network devices. Removing this VIB may impact the network connectivity based on how you make use of this device in your environment.
scsi-bnx2fc	This is a driver package used to initialize Broadcom Fiber channel devices. Removing this VIB may impact the fibre channel LUN connectivity based on how you make use of this device in your environment.
net-qlge	This is driver package used to enable Qlogic 10G network devices. Removing this VIB may impact the network connectivity based on how you make use of this device in your environment.

scsi-bnx2i	This is driver package used for enable Broadcom iSCSI devices. Removing this VIB may impact the iSCSI connectivity based on how you make use of this device in your environment.
lsu-mptsas-plugin	This is a plugin package used for mptsas driver based storage devices.
sata-ahci	This is a driver package used to enable AHCI onboard SATA devices. Removing this VIB may impact the SATA devices availability based on how you make use of this device in your environment.

References

- VMware Blog on UEFI Secureboot
- Dell white paper on VMware ESXi and UEFI Secureboot
- VMware documentation on UEFI Secureboot
- UEFI Spec