VMware ESXi Secureboot for Dell PowerEdge Servers

ABSTRACT
This paper explains UEFI secureboot feature enabled from VMware ESXi 6.5 for Dell PowerEdge servers.

November, 2016

Gobind Vijayakumar
Krishnaprasad K
Table of Contents

INTRODUCTION TO UEFI SECUREBOOT ........................................................................................................3
AUDIENCE AND SCOPE ...................................................................................................................................4
SECUREBOOT IN VMWARE ESXI ........................................................................................................................4
DELL SUPPORT FOR UEFI SECUREBOOT ........................................................................................................6
STEPS TO ENABLE UEFI SECUREBOOT IN DELL POWEREDGE SERVERS ..................................................6
UTILITIES IN VMWARE ESXI FOR SECUREBOOT ..........................................................................................7
SECUREBOOT FOR VIRTUAL MACHINES ........................................................................................................7
TROUBLESHOOTING .......................................................................................................................................8
REFERENCES ....................................................................................................................................................10

Figure 1 : UEFI Secureboot Overview ................................................................................................................3
Figure 2 : Secureboot flow in VMware ESXi ........................................................................................................5
Figure 3 : BIOS Setup Page to manage SECUREBOOT ......................................................................................6
Figure 4 : VMware CA in System Firmware .......................................................................................................6
Figure 5 : UEFI Secure Boot in Progress during VMware ESXi Boot ..................................................................7
Figure 6 : Command validating the image profile VIBs ......................................................................................7
Figure 7 : Command to check the status of UEFI Secure Boot in VMware ESXi ................................................7
Figure 8 : Signature verification failure PSOD ....................................................................................................9
Figure 9 : UEFI Secure Boot Error Code 39 .......................................................................................................10
Introduction to UEFI Secureboot

UEFI secure boot is a feature described by the UEFI specification (2.3.1c) which is available from the UEFI Forum Site. Secure Boot uses a database of digital signatures to validate the integrity of firmware, the operating system, or UEFI drivers. These digital signatures must be generated using a special signing certificate from a specific Certificate Authority. When an executable like a boot loader or Option ROM is discovered, the UEFI checks if:

– The executable is signed with an authorized key, or
– The key, signature, or hash of the executable is stored in the authorized signature database.

If the firmware doesn’t match a digital signature, the computer won’t boot until signed firmware is restored.

Figure 1: UEFI Secureboot Overview
**Audience and Scope**

This white paper is intended for users who plan to use UEFI secureboot on Dell PowerEdge servers with VMware ESXi installed. It talks about a high level flow of UEFI secureboot in VMware ESXi followed by the settings required in the system firmware to enable it. This paper covers some of the utilities that would be useful in checking the status of secureboot in ESXi. This also talks about some of the troubleshooting options which can be useful when users come across some of the known error codes.

**Secureboot in VMware ESXi**

From ESXi 6.5, VMware introduced support for UEFI secureboot. UEFI secureboot in general verifies the integrity of each and every package loaded as part of OS bootup. In the case of VMware ESXi, secureboot verifies the integrity of VIB package(s) loaded from the boot device.

A high level flow of how secureboot works in ESXi is as below.
The mboot boot loader in ESXi contains a VMware public key and is validated against the CA present in the platform BIOS UEFI secureboot authorized database (DB) during ESXi boot. The boot loader uses this key to verify the signature of the kernel and a small subset of the system that includes a secure boot VIB verifier - a package which is used for validating the signature of the drivers and other VIB packages loaded from the boot device. If any of the VIB(s) installed on ESXi does not match the signature with the public key contained in the bootloader, ESXi boot ends up in a Purple Screen Of Death (PSOD) mentioning the signature mismatch for the specific VIBs which failed.

The 13th generation of Dell server BIOS already carries the VMware CA in the UEFI secureboot authorized database (DB). You should download the latest server BIOS from Dell support page before enabling UEFI secureboot.
**Dell support for UEFI secureboot**

Dell support UEFI secureboot from their 13th generation of PowerEdge servers only. VMware support secureboot from ESXi 6.5 onwards.

**Steps to enable UEFI secureboot in Dell PowerEdge Servers**

UEFI secureboot is available from Dell’s 13th generation of servers as indicated above. Set the Boot Mode to UEFI as the default mode would be BIOS. Save the setting and restart the server and boot back to the BIOS setup page again. Traverse to ‘System Security’ section and move onto ‘SECURE BOOT’ option at the end of the page.

The Secure Boot Policy option is set as Standard by default. Enable the Secure Boot option and set the policy to ‘Standard’.

![Figure 3: BIOS Setup Page to manage SECUREBOOT](image)

In ‘Secure Boot Policy Summary’ link, you may observe that VMware CA is present in the UEFI authorized signature database entries (DB). A sample entry is as below.

```
<table>
<thead>
<tr>
<th>Type</th>
<th>X.509 Certificate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Issuer</td>
<td>/C=US/ST=California/L=Palo Alto/O=VMware, Inc.</td>
</tr>
<tr>
<td>Subject</td>
<td>/C=US/ST=California/L=Palo Alto/O=VMware, Inc.</td>
</tr>
<tr>
<td>Signature Owner GUID</td>
<td>A3D5E95B-0A8F-4753-8735-445AFB708F62</td>
</tr>
</tbody>
</table>
```

![Figure 4: VMware CA in System Firmware](image)
Setup a password for System Password and Setup Password as notified while turning on secure boot. Once the settings are saved, booting into ESXi shows that ‘UEFI Secure Boot in progress’.

![Image of UEFI Secure Boot in Progress during VMware ESXi Boot](image)

There are few utilities provided by VMware to check the status of secureboot in ESXi. The next section talk about them in detail.

**Utilities in VMware ESXi for secureboot**

VMware provides a python program to check if the host is capable for secureboot. The program validates signature of each packages installed on ESXi to see if it’s verified and matched with the public key present in the ESXi boot loader. The below are the command line options to verify the VIB package signatures and to check the status of secureboot.

**NOTE:** It’s highly recommended to run the below program to see if the packages installed in ESXi is capable of supporting secureboot before turning on secureboot from the system BIOS.

```
[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 tskids validated. All acceptance levels validated
```

![Figure 6: Command validating the image profile VIBs](image)

```
[root@he-dhcp-100-98-14-74:] /usr/lib/vmware/secureboot/bin/secureBoot.py -s
Enabled
```

![Figure 7: Command to check the status of UEFI Secure Boot in VMware ESXi](image)

**Secureboot for Virtual Machines**

VMware ESXi 6.5 support secureboot for virtual machines as well. Pre-Requisites to check before deploying the Guest OS are as follows.

- Virtual machine Hardware Version should be 13
- Virtual machine boot mode should be set to EFI.
- Enable Secure Boot in 'Boot Options' under 'VM Options'. From command line point of view, add the following to the VM’s .vmx file.
  - `firmware = "efi"uefi.secureBoot.enabled = "TRUE"`

VMware ESXi Secureboot for Dell PowerEdge Servers
To make sure that secureboot is enabled for the guest operating system, check the log file vmware.log for the corresponding virtual machine. As an example, the following entries would be logged if all goes well.

```
vcpu-0| I125: SECUREBOOT: Signature: 1 in db, 0 in dbx, 0 unrecognized, 0 unsupported alg. Hash: 0 in db, 0 in dbx.
vcpu-0| I125: SECUREBOOT: Image APPROVED.
```

**Troubleshooting**

1. The below is a command line utility helps to check if the system firmware boot mode is set to UEFI/BIOS.

   - `vsish -e get /hardware/firmwareType` helps to check if the system BIOS boot mode is set to UEFI or BIOS. If this returns ‘1’, the system is booted in UEFI mode and if it returns ‘0’, it’s set to BIOS mode.

   - For example, if an ESXi package (VIB or driver) has been tampered with, a purple screen with the following message appears when secureboot is enabled in system BIOS.
     
     ```
     UEFI Secure Boot failed: Failed to verify signatures of the following vib(s) : [VIB Names]
     ```

   - For example, when a user upgrades from Dell customized 6.0 U2 A03 to 6.5 A00, the bootup ends up in a PSOD as follows if secureboot is enabled.

2. If UEFI secure boot is disabled in system BIOS, only a Sysalert is generated instead of PSOD in case a signature mis match is found for any of the packages installed. If UEFI SecureBoot is enabled in system BIOS and if there is any break in the chain of root trust, bootup results in a signature mismatch PSOD.

   - For example, if an ESXi package (VIB or driver) has been tampered with, a purple screen with the following message appears when secureboot is enabled in system BIOS.

   ```
   UEFI Secure Boot failed: Failed to verify signatures of the following vib(s) : [VIB Names]
   ```
Hence the recommendation is to run the python program (as indicated in ‘Utilities in VMware ESXi for secureboot’ section) prior to enabling secureboot from platform BIOS. In this specific case, user can explicitly remove the drivers tg3, qlge as they are not required for ESXi 6.5. There are other drivers replacing these two in 6.5. The lsu-lsi-mptsas-plugin also can be removed using “esxcli software vib remove –n <VIB ID>” command. Refer to a white paper posted by Dell named Upgrade guide for Dell customized VMware ESXi 6.5 which detail on the Upgrade Scenarios from Dell customized images point of view. Also refer to VMware KB which talks about some of the secureboot failing scenarios interms of ESXi upgrade from previous versions.

3. Another example error code is FATAL error 39. This generally happens when the kernel is tampered and when it doesn’t match with the boot loader Public key.
References

- vSphere Security guide for ESXi 6.5
- Cannot enable secure boot on ESXi 6.5 host that was upgraded (2147606)
- How to Enable UEFI Secure Boot on VMware ESXi 6.5.x – A video blog