Lenovo

A Technical Introduction to the Use of Trusted Platform Module 2.0 with VMware vSphere 6.7

Introduces the features of TPM 2.0

Explains the prerequisites for using TPM 2.0 on vSphere 6.7

Shows how to configure and use TPM in vSphere 6.7

Shows the equivalent OneCLI commands for automation

Chengcheng Peng

LENOVO PRESS

Abstract

Trusted Platform Module (TPM 2.0) is an international standard for a secure cryptoprocessor, which is a dedicated microcontroller designed to secure hardware through integrated cryptographic keys. From laptops to desktops to servers, TPM 2.0 chips are found in most of today's computers. Currently, TPM 2.0 chips are also available on Lenovo® ThinkSystem™ servers as well as most of the Lenovo System x, ThinkServer, and Flex System product families.

This document presents a briefly technical overview of the TPM 2.0 and describes how to configure and use TPM 2.0 in VMware vSphere 6.7 on Lenovo servers. This document is intended for IT administrators who are familiar with TPM 2.0 and VMware ESXi 6.7 and vCenter 6.7.

At Lenovo Press, we bring together experts to produce technical publications around topics of importance to you, providing information and best practices for using Lenovo products and solutions to solve IT challenges.

See a list of our most recent publications at the Lenovo Press web site:

http://lenovopress.com

Do you have the latest version? We update our papers from time to time, so check whether you have the latest version of this document by clicking the **Check for Updates** button on the front page of the PDF. Pressing this button will take you to a web page that will tell you if you are reading the latest version of the document and give you a link to the latest if needed. While you're there, you can also sign up to get notified via email whenever we make an update.

Contents

Introduction

Trusted Platform Module (TPM 2.0) is a standard secure microprocessor that can securely store artifacts used to authenticate the platform. TPM 2.0 is designed to offer comprehensive protections based on hardware roots of trust and also offer the flexibility for industry implementations across a broad range of platforms including servers, desktops, embedded systems, mobile devices and network equipment. TPM 2.0 devices are now available from many vendors. Lenovo servers currently offer the Nuvoton TPM and Nationz TPM.

The goal for TPM 2.0 is to replace the TPM 1.2 standard because of various limitations in TPM1.2. Note that TPM 2.0 and TPM 1.2 are two entirely different implementations and there is no backwards compatibility.

Architecture overview

TPM 2.0 has introduced many new concepts and features, including crypto-agility, easier management, a more flexible authorization model, and better extensibility.

Figure 1 shows the overall architecture of the TPM 2.0 and the functional units required for its operation.

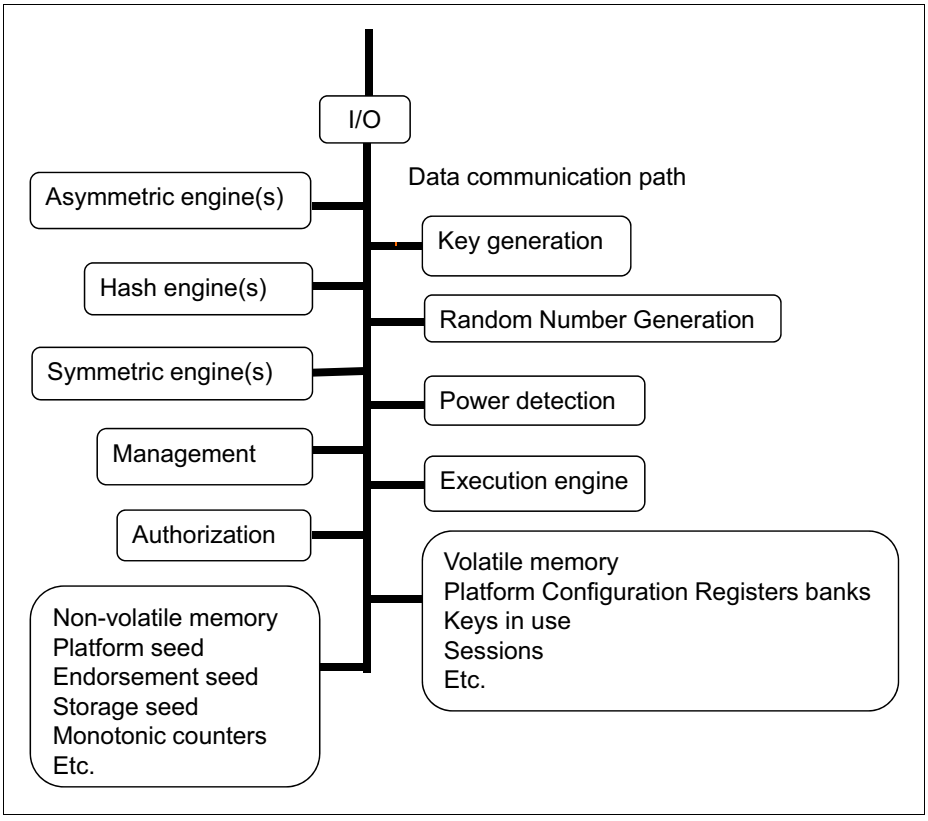

Figure 1 TPM 2.0 architectural overview

Software stack

The TPM 2.0 software stack provides an API that allows applications and the operating system to use the TPM. It is developed to be compliant with the most recent TCG v1.38 specification and compatible with any TPM 2.0 implementation.

Figure 2 shows the overview of TPM 2 software stack.

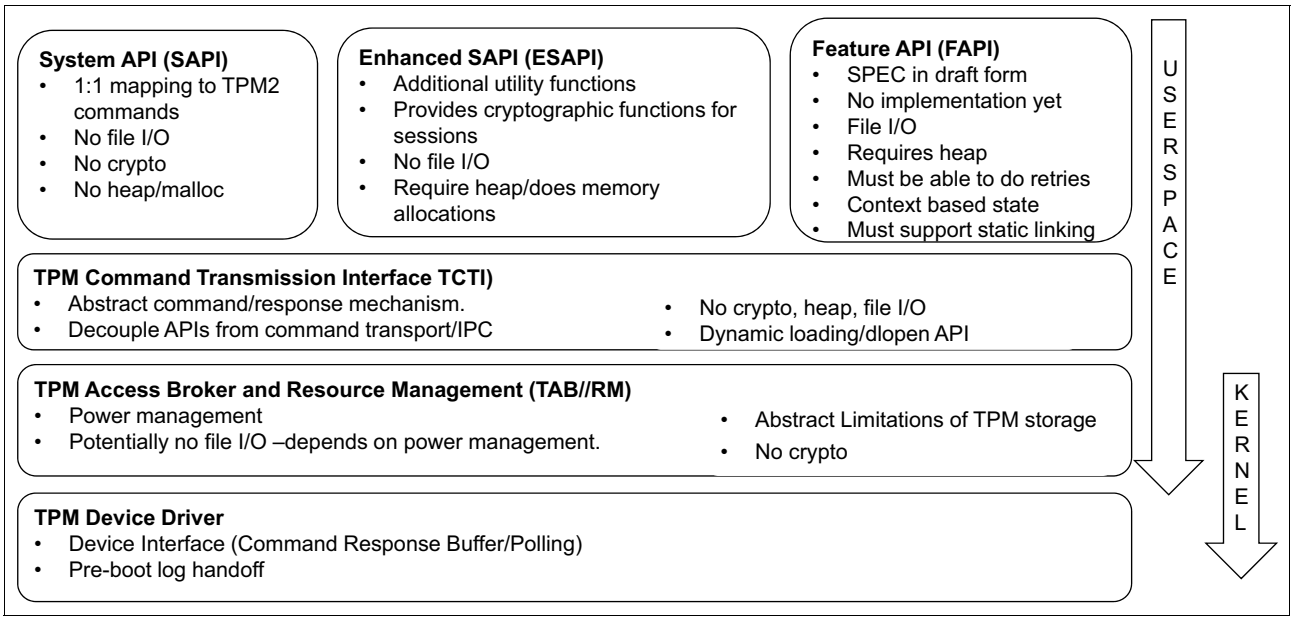

Figure 2 TPM 2.0 software stack

TPM 2.0 support

TPM 2.0 supports a variety of algorithm as shown in Table 1.

Table 1 TPM 2.0 supported cryptographic algorithms

Algorithm type	Algorithm name	TPM 2.0
Asymmetric	RSA 1024	Yes
	RSA 2048	Yes
	ECC P256	Yes
	ECC P256	Yes
Symmetric	AES 128	Yes
	AES 256	No
Hash	SHA-1	Yes
	SHA-2 256	Yes
HMAC	SHA-1	Yes
	SHA-2 256	Yes

TPM 2.0 supports a variety Hierarchy, Root keys, Authorization and NV RAM specifications as shown in Table 2.

Table 2 TPM 2.0 supported Hierarchy, Root Keys, Authorization and NV RAM

Specification	TPM 2.0
Hierarchy	Support platform, storage and endorsement
Root Keys	Support multiple keys and algorithms per hierarchy
Authorization	Support password, HMAC, and policy (which covers HMAC, PCR, locality, and physical presence).
NV RAM	Support unstructured data, Counter, Bitmap, Extend

Dependency and version compatibility

Intel Trusted Execution Technology (Intel TXT) make use of TPM to strengthen security of system. This section introduces the dependency of Intel TXT, TPM 2.0 and UEFI Secure Boot and also introduces which vSphere versions support these security technologies.

Intel TXT and UEFI Secure Boot

Intel Trusted Execution Technology (Intel TXT) is computer hardware technology that uses a TPM and cryptographic techniques to provide measurements of software and platform components so that the system software and management applications may use those measurements to make trust decisions. TPM is a dependency of Intel TXT, because the TPM is where TXT will store the measurements of the platform.

Unified Extensible Firmware Interface (UEFI) is a replacement for the traditional BIOS firmware that has its roots in the original IBM PC. In UEFI parlance, Secure Boot is a protocol of the UEFI firmware and this capability is designed to ensure that boot loaders are not compromised by validating their digital signature against a digital certificate in the firmware.

UEFI Secure Boot is a prerequisite for TPM 2.0 support in vSphere ESXi 6.7 and later.

Version compatibility in vSphere

vSphere support is as follows:

- Starting with vSphere 6.7 U1, TPM 2.0 and Intel TXT are fully supported together.
- vSphere 6.7 base supports TPM 2.0, however 6.7 base does not use Intel TXT in conjunction with TPM 2.0. Intel TXT is not used and the setting in UEFI for Intel TXT is ignored.
- vSphere 6.5 and earlier ignores the TPM 2.0 hardware and ignores any attempt to enable and use Intel TXT trusted boot.

Table 3 shows the vSphere versions and TPM/Intel TXT/Secure Boot support matrix.

Table 3 vSphere version and TPM/TXT/Secure Boot support matrix

vSphere version	TPM/Intel TXT options	Is UEFI Secure Boot required?
vSphere 6.0 to vSphere 6.5	TPM 1.2 with Intel TXT	No
vSphere 6.7 base	TPM 1.2 with Intel TXT	No
	TPM 2.0	Yes

vSphere version	TPM/Intel TXT options	Is UEFI Secure Boot required?
vSphere 6.7 U1 or later	TPM 1.2 with Intel TXT	No
	TPM 2.0	Yes
	TPM 2.0 with Intel TXT	Yes

Configuring and using TPM 2.0 in vSphere 6.7

This section describes the steps how to configure TPM 2.0 for use with vSphere 6.7.

In order to use TPM 2.0, the vCenter Server environment must meet the following requirements:

- vCenter Server 6.7 or newer version.
- ESXi 6.7 or newer version host with TPM 2.0 chip installed and correctly configured in UEFI.
- UEFI Secure Boot enabled.

Server UEFI settings

Correctly configuring the TPM 2.0 chip in the UEFI setting involves ensuring a number of settings are correct. The following are steps for configuring UEFI.

1. Select **UEFI Mode** as System Boot Mode.
2. Enable UEFI Secure Boot.
3. Make sure that TPM 2.0 chip is installed and shown in UEFI setting.

   The TPM 2.0 is set to use SHA-256 hashing and use the IS/FIFO (First-In, First-Out) interface by default on Lenovo servers. VMware vSphere requires TPM 2.0 is set to use SHA-256 hashing and use the IS/FIFO interface, so you may need to manually set it on other vendor servers.
4. Enable Intel TXT if you want to use Intel TXT function with TPM 2.0. In order for Intel TXT to function properly the following are prerequisites:
   - Intel Xeon processor-based server platform with Intel TXT Enabled UEFI.
   - Intel Virtualization Technology (Intel VT) must be enabled.
   - Intel Virtualization Technology with Directed I/O (Intel VT-d) must be enabled.
   - A Trusted Platform Module (TPM1.2/TPM 2.0) must be enabled and activated.
   - A ThinkSystem server or another server where Intel SINIT authenticated code module (ACM) is installed and enabled in UEFI.
   - A hypervisor that supports trusted boot (t-boot). VMware vSphere ESXi6.7 is one of the hypervisor that support trusted boot.

Configuration procedures

The following are steps for configuring and using TPM 2.0 in vSphere 6.7 U1 on a ThinkSystem SR630 server.

1. Power on the Lenovo server and press F1 when prompted to enter System Setup, Figure 3.

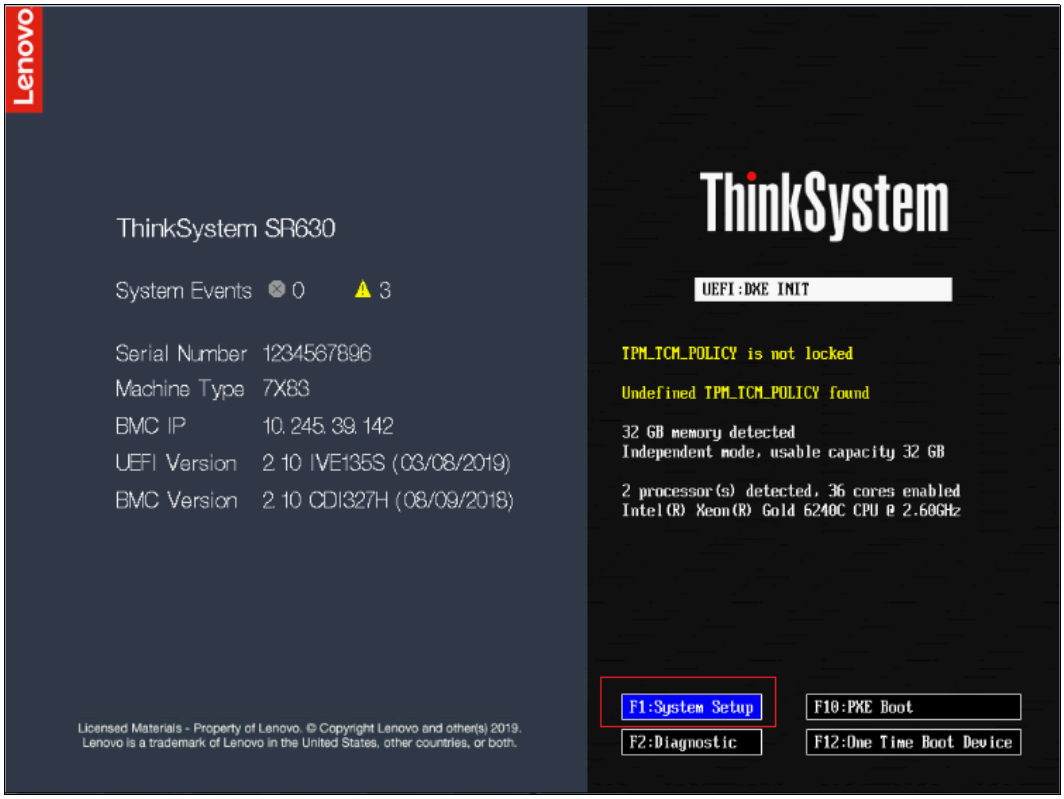

Figure 3 Press F1 to enter System Setup

2. Select **UEFI Mode** as System Boot Mode in UEFI Setting.
   a. On the System Configuration and Boot Management page, choose **Boot Manager** → **Boot Modes** → **System Boot Mode**,
   b. Set System Boot Mode to **UEFI Mode** as shown in Figure 4 on page 8.

Figure 4 Boot Modes page on Lenovo ThinkSystem SR630 server

3. Assert Physical Presence as follows:

Tip: Secure Boot Settings and Secure Boot Policy are modifiable when Physical Presence is asserted. Physical Presence is a form of authorization to perform certain security functions. *Asserted* means being *authorized*. So we need to make sure that hardware Physical Presence is asserted before we can enable Secure Boot.

a. Login to the XClarity Controller web interface

b. Click **BMC Configuration** → **Security** → **Assert Physical Presence**. Figure 5 on page 9 appears.

c. Click the **Assert** button and click **Apply** to assert Physical Presence.

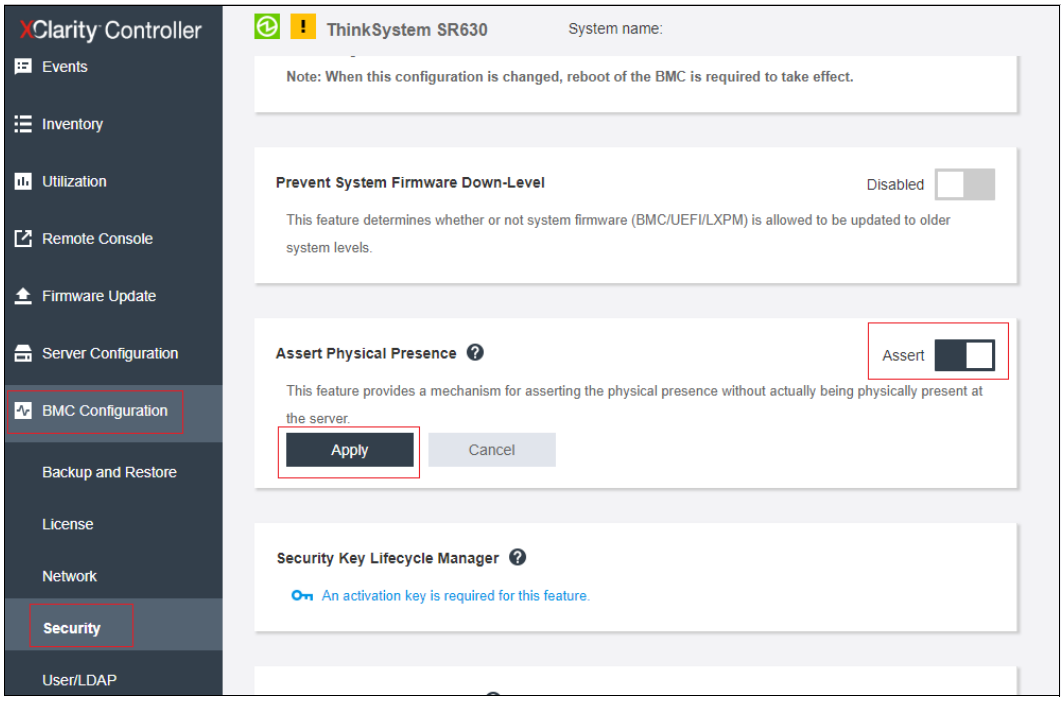

Figure 5 Assert physical presence

4. Enable UEFI Secure Boot in UEFI settings as follows:
   a. In System Setup, navigate to the System Configuration and Boot Management page.
   b. Select **System Settings** → **Security** → **Secure Boot Configuration**.
   c. Enable secure boot setting as shown in Figure 6.

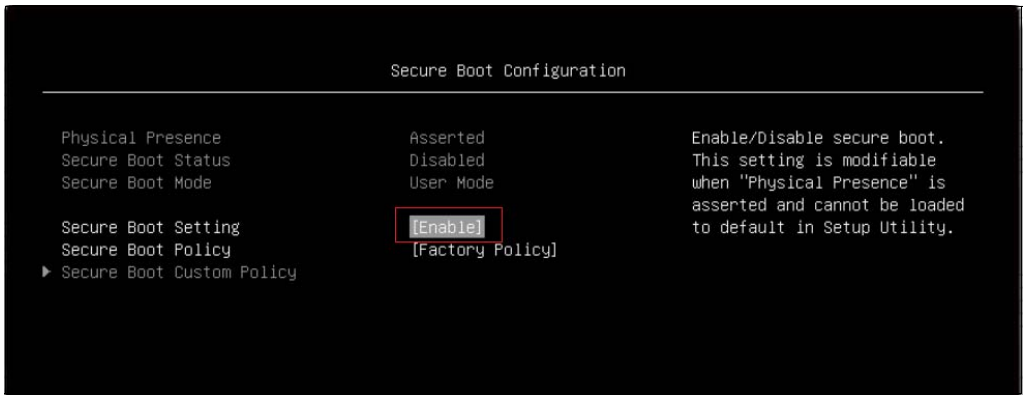

Figure 6 Secure Boot settings

5. Enable TPM 2.0 in UEFI, as follows:
   a. In System Setup, navigate to the System Configuration and Boot Management page
   b. Select **System Settings** → **Security** → **Trusted Platform Module** → **Update to TPM2.0 compliant**, toggling to TPM 2.0. See Figure 7 on page 10

Figure 7 TPM page in System Setup

c. Select **TPM 2.0** as shown and press Enter to display the TPM 2.0 page, where you can view the TPM vendor, TPM firmware version, and TPM physical presence status, as shown in Figure 8. You can also clear all TPM data from this page.

Figure 8 TPM 2.0 details

6. Enable Intel TXT if you want to use Intel TXT function together with TPM 2.0, as follows:
   a. In System Setup, select **System Settings** → **Processors**
   b. Select Trusted Execution Technology and press Enter to enable the function, as shown in Figure 9 on page 11

Tip: Intel Virtualization Technology (Intel VT) and Intel Virtualization Technology with Directed I/O (Intel VT-d) have already been enabled by default on Lenovo servers

Figure 9 Enable Intel TXT

7. install VMware ESXi on the server
8. Deploy vCenter
9. Boot into the ESXi host and run the following command to confirm that Secure Boot is enabled.

   ~# /usr/lib/vmware/secureboot/bin/secureBoot.py -c
   ~# /usr/lib/vmware/secureboot/bin/secureBoot.py -s

   Figure 10 shows the output of the commands. The **-c** parameter checks whether Secure Boot can be enabled or not, and the **-s** parameter displays the current status of Secure Boot.

```
[root@localhost:~] /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@localhost:~] /usr/lib/vmware/secureboot/bin/secureBoot.py -s
Enabled
```

Figure 10 Output of secureBoot check

10. Run the following command to check present status and version of the TPM chip.

    ~# vsish -e get /hardware/tpm/present
    ~# vsish -e get /hardware/tpm/version

Figure 11 shows the output of TPM check command. The output of `1` means the TPM chip is present in the system. The output of `2` means the version is TPM 2.0.

```
[root@localhost:~] vsish -e get /hardware/tpm/present
1
[root@localhost:~] vsish -e get /hardware/tpm/version
2
```

Figure 11 Output of TPM chip present and version

11. Run the following command to check the status of trustedboot.

    ~# esxcli hardware trustedboot get

    Figure 12 shows the output of trustedboot check command for ESXi 6.7 GA build when Intel TXT is enabled. ESXi 6.7 GA (base) does not support Intel TXT work together with TPM 2.0, so the output of `Drtm Enabled: false` in ESXi 6.7 GA is expected.

```
[root@localhost:~] esxcli hardware trustedboot get
   Drtm Enabled: false
   Tpm Present: true
```

Figure 12 Output of trustedboot status in ESXi 6.7 GA

Figure 13 shows the output of trustedboot check command for ESXi6.7 U1 and newer version when Intel TXT is enabled. ESXi 6.7 U1 adds support Intel TXT work together with TPM 2.0, so it shows `Drtm Enabled: true`.

```
[root@localhost:~] esxcli hardware trustedboot get
   Drtm Enabled: true
   Tpm Present: true
```

Figure 13 Output of trustedboot status in ESXi 6.7 U1

12. Run the following commands to check TPM driver:

    ~ # vmkload_mod -l |grep tpm
    ~ # zcat /var/log/boot.gz | grep -i -E "tpm"

    Figure 14 shows the output of the command `vmkload_mod -l |grep tpm`:

```
[root@localhost:~] vmkload_mod -l |grep tpm
tpmdriver                    2     120
```

Figure 14 The output of check TPM driver

Figure 15 on page 13 shows the output of the command `zcat /var/log/boot.gz | grep -i -E "tpm"`. The highlighted text in the figure is the portion of the output that you should check for the TPM driver.

```
[root@localhost:~] zcat /var/log/boot.gz | grep -i -E "tpm"
VMB: 183: TPM IO address found is unset, using default 0xfed40000
VMB: 603: TPM is in FIFO mode.
VMB: 1596: Initialization of TPM 2 impl done.
VMB: 89: injectPMemSratEntries = FALSE
TSC: 897038 cpu0:1)BootConfig: 806: injectPMemSratEntries = FALSE
ACPI: TPM2 0xa6e2db60 00034 (v03 LENOVO THINKSYS 00000100      01000013)
0:00:00:04.809 cpu0:2097152)VMKAcpi: 390: \_SB_.TPM_: found VMKAPI-capable ACPI PNP Device.
0:00:00:04.815 cpu0:2097152)Device: 1466: Registered device: 0x43053b8b1410 \_SB_.TPM_
h07NTN1003x08MSFT0101 (parent=0x2a9343053b8b16a4)
0:00:00:04.815 cpu0:2097152)VMKAcpi: 699: \_SB_.TPM_: registered VMKAPI-capable ACPI PNP Device
(h07NTN1003x08MSFT0101).
0:00:00:04.834 cpu0:2097152)TPM FixedMem: start = 0xfed40000, end = 0xfed44fff, write protect = 1
2019-10-15T05:29:23.718Z cpu7:2097545)Activating Jumpstart plugin tpm.
2019-10-15T05:29:23.791Z cpu10:2098149)Loading module tpmdriver ...
2019-10-15T05:29:23.793Z cpu10:2098149)Elf: 2101: module tpmdriver has license VMware
2019-10-15T05:29:23.807Z cpu10:2098149)TPM FixedMem: start = 0xfed40000, end = 0xfed44fff, write protect
= 1
2019-10-15T05:29:23.817Z cpu10:2098149)TPM FixedMem: start = 0xfed40000, end = 0xfed44fff, write protect
= 1
2019-10-15T05:29:23.817Z cpu10:2098149)tpmDriver: TpmDriverFindIoMemory:332: Found TPM at base:
0xfed40000
2019-10-15T05:29:23.817Z cpu10:2098149)tpmDriver: Tpm2Init:1582: Activated locality 2
2019-10-15T05:29:23.817Z cpu10:2098149)tpmDriver: Tpm2CheckInterface:603: TPM is in FIFO mode.
2019-10-15T05:29:23.828Z cpu10:2098149)tpmDriver: Tpm2Init:1596: Initialization of TPM 2 impl done.
2019-10-15T05:29:23.838Z cpu10:2098149)tpmDriver: Tpm2LogVendor:1551: Vendor ID: NTC
2019-10-15T05:29:23.881Z cpu10:2098149)tpmDriver: Tpm2ResMgr_Init:1415: TPM 2.0 Resource manager
initialized.
2019-10-15T05:29:23.923Z cpu10:2098149)Mod: 4962: Initialization of tpmdriver succeeded with module ID
78.
2019-10-15T05:29:23.923Z cpu10:2098149)tpmdriver loaded successfully.
2019-10-15T05:29:23.931Z cpu7:2097545)Jumpstart plugin tpm activated.
[root@localhost:~]
```

Figure 15 The TPM driver related log in boot.gz

The TPM driver on ESXi may fail to load and report errors with error code 0x921 or 0x98e in vmkernel.log. This kind of issue is caused if another operating system has previously taken ownership of the TPM. By design, TPM driver on ESXi does not overwrite the ownership of the TPM on the server platform. To resolve this error, clear the TPM chip data using the UEFI setting shown in Figure 8 on page 10.

Figure 16 shows the similar error code 0x921/0x98e in vmkernel.log.

```
[root@IMM2-6cae8b2beba5:~] 2018-05-23T15:58:32.037Z
cpu112:2100954)tpmDriver: Tpm2ResMgrProcessResponse:846: Error: TPM command
error code 0x921/0x98e
```

Figure 16 TPM error code 0x921/0x98e in vmkernel.log

13. Create a datacenter and cluster on the vCenter server, and then add the ESXi server to the vCenter server. Figure 17 shows add ESXi host to vCenter server cluster.

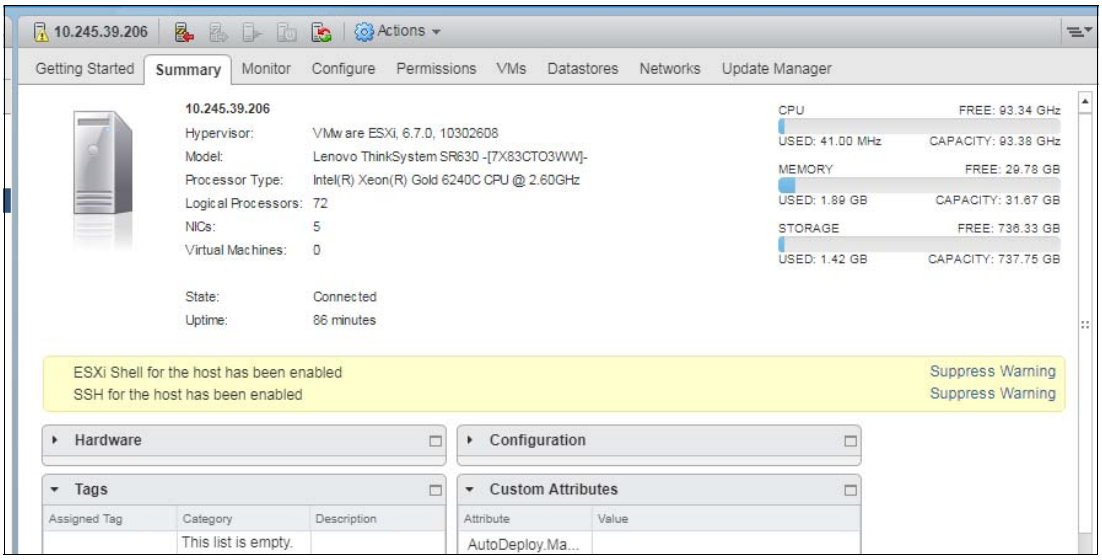

Figure 17 Add ESXi host to vCenter server cluster

14. Check ESXi host attestation status as follows. The expected status is that no host TPM attestation alarm is reported.
    a. Connect to vCenter Server by using the vSphere Client.
    b. Navigate to a Datacenter and click the Monitor tab.
    c. Click “Issues” -> “Triggered Alarms”.
    d. Review the host's status in the Attestation column and read the accompanying message in the Message column:
        - No host TPM attestation alarm: indicating full trust, TPM attestation success.
        - Red host TPM attestation alarm: TPM attestation failed.

    Figure 18 shows there’s no host TPM attestation alarm when TPM attestation success.

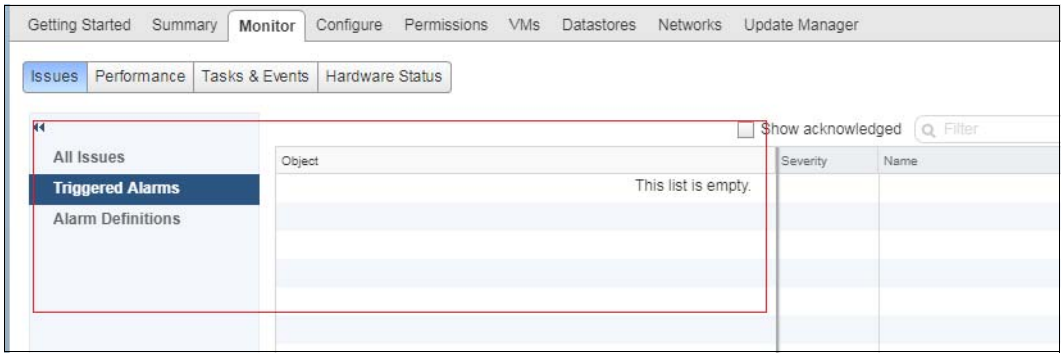

Figure 18 No host TPM attestation alarm

Figure 19 shows the host TPM attestation alarm on Summary page when TPM attestation failed.

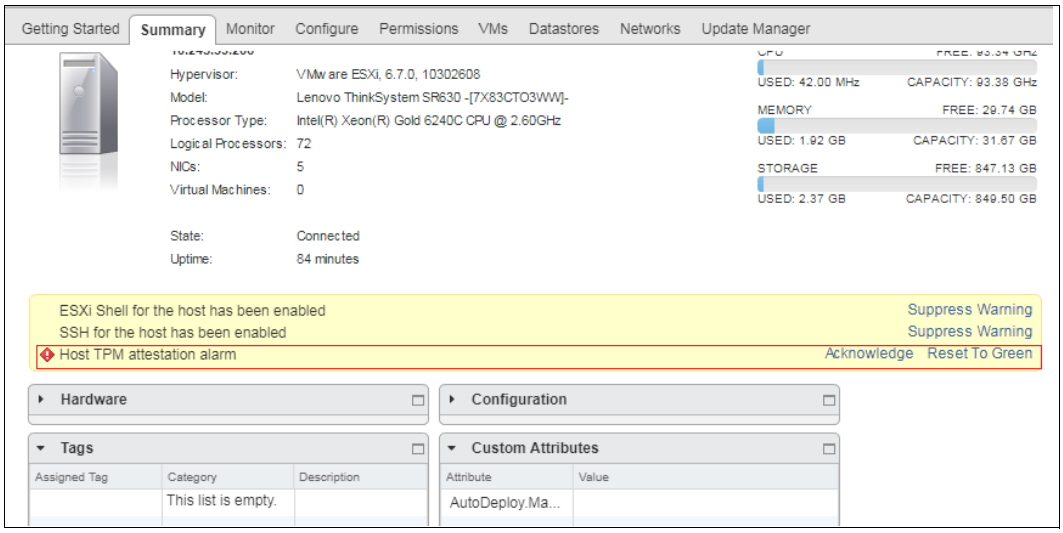

Figure 19 TPM attestation alarm on Summary page

Figure 20 shows the host TPM attestation alarm on Triggered Alarms page when TPM attestation failed.

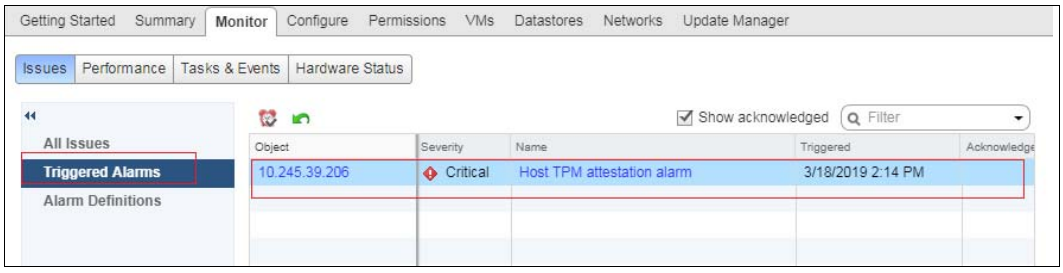

Figure 20 TPM attestation alarm on Triggered Alarms page

Using OneCLI to configure TPM 2.0

Lenovo XClarity™ Essentials OneCLI is a collection of command-line utilities which can be used to configure the server, collect service data for the server, update firmware and device drivers, and perform power-management functions on the server. OneCLI is especially useful if you wish to automate certain processes. This section shows examples on how to configure TPM 2.0-related settings using OneCLI.

You can download OneCLI from the Lenovo support site:

https://datacentersupport.lenovo.com/us/en/solutions/ht116433

The OneCLI commands to configure TPM 2.0 are as follows:

1. Assert Physical Presence and check the status of Physical Presence.

   Run the following OneCLI command to assert Physical Presence:

   ```
   OneCli.exe config set
   PhysicalPresencePolicyConfiguration.PhysicalPresencePolicy Enable --imm
   <USERID>:<PASSWORD>@<IP>
   ```

Figure 21 shows an example on how to assert Physical Presence via OneCLI command.

```
D:\onecli>OneCli. exe config set
PhysicalPresencePolicyConfiguration.PhysicalPresencePolicy Enable --imm
USERID :PASSWORD@10.245.39.142
...
Invoking SET command ...
Connected to BMC at IP address 10.245.39.142 by IPMI
PhysicalPresencePolicyConfiguration.PhysicalPresencePolicy=Enable
Success.
```

Figure 21 Assert Physical Presence via OneCLI command

Run the following OneCLI command to check the status of Physical Presence:

```
OneCli.exe config show
PhysicalPresencePolicyConfiguration.PhysicalPresencePolicy –imm
<USERID>:<PASSWORD>@<IP>
```

Figure 22 shows an example on how to check the status of Physical Presence via OneCLI command.

```
D:\onecli>OneCli.exe config show
PhysicalPresencePolicyConfiguration.PhysicalPresencePolicy --imm
USERID:PASSWORD@10.245.39.142
...
Invoking SHOW command ...
Connected to BMC at IP address 10.245.39.142 by IPMI
PhysicalPresencePolicyConfiguration.PhysicalPresencePolicy=Enable
Success.
```

Figure 22 Check status of Physical Presence via OneCLI command

2. Enable Secure Boot and check the status of Secure Boot.

   Run the following OneCLI command to enable Secure Boot:

   ```
   OneCli.exe config set SecureBootConfiguration.SecureBootSetting Enabled
   --override --imm <USERID>:<PASSWORD>@<IP>
   ```

   Figure 23 shows an example on how to enable Secure Boot via OneCLI command.

```
D:\onecli>OneCli.exe config set SecureBootConfiguration.SecureBootSetting
Enabled --override --imm USERID:PASSWORD@10.245.39.142
...
Invoking SET command ...
Connected to BMC at IP address 10.245.39.142 by IPMI
SecureBootConfiguration.SecureBootSetting=Enabled
Success.
```

Figure 23 Enable Secure Boot via OneCLI command

Run the following OneCLI command to check the status of Secure Boot:

```
OneCli.exe config show SecureBootConfiguration.SecureBootSetting --imm
<USERID>:<PASSWORD>@<IP>
```

Figure 24 shows an example on how to check status of Secure Boot via OneCLI command.

```
D:\onecli>OneCli.exe config show SecureBootConfiguration.SecureBootSetting
--imm USERID:PASSWORD@10.245.39.142
...
Invoking SHOW command ...
Connected to BMC at IP address 10.245.39.142 by IPMI
SecureBootConfiguration.SecureBootSetting=Enabled
Success.
```

Figure 24 Check status of Secure Boot via OneCLI command

3. Update TPM 1.2 to TPM 2.0.

   Run the following OneCLI command to update TPM 1.2 to TPM 2.0:

   ```
   OneCli.exe config set TrustedComputingGroup.DeviceOperation "Update to TPM2.0
   compliant" --override --imm <USERID>:<PASSWORD>@<IP>
   ```

   Figure 25 shows an example on how to update to TPM 2.0 compliant via OneCLI command.

```
D:\onecli>OneCli. exe config set TrustedComputingGroup.DeviceOperation
"Update to TPM2.0 compliant" --override --imm USERID:PASSWORD@10.245.39.142
...
Invoking SET command ...
Connected to BMC at IP address 10.245.39.142 by IPMI
TrustedComputingGroup.DeviceOperation=Update to TPM2. 0 compliant
Success.
```

Figure 25 Update to TPM 2.0 compliant via OneCLI command

   Run the following OneCLI command to check the status of TPM device:

   ```
   OneCli.exe config show TrustedComputingGroup.DeviceStatus –imm
   <USERID>:<PASSWORD>@<IP>
   ```

   Figure 26 shows an example on how to check the status of TPM device via OneCLI command.

```
D:\onecli>OneCli.exe config show TrustedComputingGroup.DeviceStatus --imm
USERID:PASSWORD@10.245.39.142
...
Invoking SHOW command ...
Connected to BMC at IP address 10.245.39.142 by IPMI
TrustedComputingGroup.DeviceStatus=TPM2.0 Device is enabled, Hardware
Physical Presence is Asserted.
Success.
```

Figure 26 Check status of TPM device via OneCLI command

4. Run the following OneCLI command to clear TPM device:

   ```
   OneCli.exe config set TrustedComputingGroup.DeviceOperation "Clear" --override
   --imm <USERID>:<PASSWORD>@<IP>
   ```

Figure 27 shows an example on how clear TPM device via OneCLI command.

```
D:\onecli>OneCli.exe config set TrustedComputingGroup.DeviceOperation
"Clear" --override --imm USERID:PASSWORD@10.245.39.142
...
Invoking SET command ...
Connected to BMC at IP address 10.245.39.142 by IPMI
TrustedComputingGroup.DeviceOperation=Clear
Success.
```

Figure 27 Clear TPM device via OneCLI command

5. Enable Intel Trusted Execution Technology (TXT) and check the status of it.

   Run the following OneCLI command to enable Intel TXT:

   ```
   OneCli.exe config set Processors.TrustedExecutionTechnology Enable --imm
   <USERID>:<PASSWORD>@<IP>
   ```

   Figure 28 shows an example on how to enable Intel TXT via OneCLI command.

```
D:\onecli>OneCli.exe config set Processors.TrustedExecutionTechnology Enable
--imm USERID:PASSWORD@10.245.39.142
...
Invoking SET command ...
Connected to BMC at IP address 10.245.39.142 by IPMI
Processors.TrustedExecutionTechnology=Enable
Success.
```

Figure 28 Enable Intel TXT via OneCLI command

   Run the following OneCLI command to check the status of Intel TXT:

   ```
   OneCli.exe config show Processors.TrustedExecutionTechnology --imm
   <USERID>:<PASSWORD>@<IP>
   ```

   Figure 29 shows an example on how to check the status of Intel TXT via OneCLI command.

```
D:\onecli>OneCli.exe config show Processors.TrustedExecutionTechnology --imm
USERID:PASSWORD@10.245.39.142
...
Invoking SHOW command ...
Connected to BMC at IP address 10.245.39.142 by IPMI
Processors.TrustedExecutionTechnology=Enable
Success.
```

Figure 29 Check status of Intel TXT via OneCLI command

References

- Review the following web pages for more information:
- Trusted Platform Module Wikipedia

  https://en.wikipedia.org/wiki/Trusted_Platform_Module

- TPM 2.0 Library Specification

  https://trustedcomputinggroup.org/resource/tpm-library-specification/
- TPM 2.0 software stack open source

  https://software.intel.com/en-us/blogs/2018/08/29/tpm2-software-stack-open-source
- VMware vSphere Documentation

  https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.security.doc/GUID-1OF7022C-DBE1-47A2-BD86-3840C6955057.html?hWord=N4IghgNiBcICoAUCyAmAdABhAXyA

Author

Chengcheng Peng is a VMware Engineer at the Lenovo Data Center Group in Beijing, China. She joined the OS team in 2018. Her main interests are vSphere security and storage. She has 5 years' experience as a VMware Engineer.

Thanks to the following specialists for their contributions and suggestions:

- Boyong Li, Lenovo OS Technical Leader
- Samer El Haj Mahmoud, Lenovo OS architect
- Steven You2 Liang, Lenovo TPM Technical Leader
- Yuepei, Lenovo OS PM
- David Watts, Lenovo Press

Notices

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area. Any reference to a Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any other product, program, or service.

Lenovo may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

Lenovo (United States), Inc.
1009 Think Place - Building One
Morrisville, NC 27560
U.S.A.
Attention: Lenovo Director of Licensing

LENOVO PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. Lenovo may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

The products described in this document are not intended for use in implantation or other life support applications where malfunction may result in injury or death to persons. The information contained in this document does not affect or change Lenovo product specifications or warranties. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Lenovo or third parties. All information contained in this document was obtained in specific environments and is presented as an illustration. The result obtained in other operating environments may vary.

Lenovo may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any references in this publication to non-Lenovo Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this Lenovo product, and use of those Web sites is at your own risk.

Any performance data contained herein was determined in a controlled environment. Therefore, the result obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

This document was created or updated on October 15, 2019.

Send us your comments via the **Rate & Provide Feedback** form found at
http://lenovopress.com/lp1234

Trademarks

Lenovo and the Lenovo logo are trademarks or registered trademarks of Lenovo in the United States, other countries, or both. These and other Lenovo trademarked terms are marked on their first occurrence in this information with the appropriate symbol (® or ™), indicating US registered or common law trademarks owned by Lenovo at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of Lenovo trademarks is available from https://www.lenovo.com/us/en/legal/copytrade/.

The following terms are trademarks of Lenovo in the United States, other countries, or both:

Lenovo®	Lenovo(logo)®
Lenovo XClarity™	ThinkSystem™

The following terms are trademarks of other companies:

Intel, Xeon, and the Intel logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Other company, product, or service names may be trademarks or service marks of others.