One-Stop Intel TXT Activation Guide

IBM® X-Series, iDataplex and BladeCenter Server Systems

Intel® Trusted Execution Technology (Intel® TXT) for Intel® Xeon processor-based servers is commonly used to enhance platform security by utilizing the underlying hardware based technology found in modern server platforms. Using a combination of the Intel Xeon processor-based and other industry leading platform technologies, such as Intel® Virtualization Technology (Intel VT), Trusted Platform Module (TPM), and appropriately configured BIOS with the Intel® SINIT ACM (authenticated code module); Intel TXT provides security against hypervisor, BIOS, firmware and other pre-launch software based attacks by establishing a 'root of trust' during the boot process. Enabling Intel TXT to protect your systems is a simple process and this will be showcased in this document.

Table of Contents

© Intel Corporation 2014

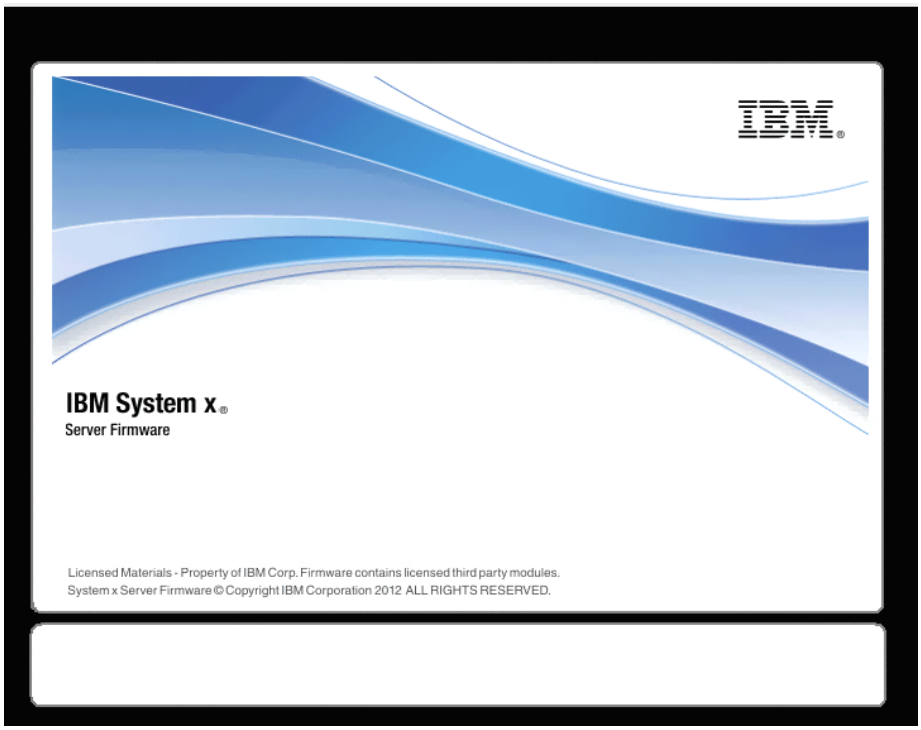
Assumptions & Guidance

- This document is intended to provide guidance for activating the TPM/Intel TXT in BIOS/uEFI console.
- As available, this document is intended to provide guidance for scale activation of TPM/Intel TXT.
- This document requires fundamental systems engineering knowledge and is intended for Systems Engineers and Systems Administrators.
- This document covers step by step instructions for two IBM X-series server platforms based on the Intel Xeon processor E5-2600 V2 family. Many IBM platforms support Intel TXT with an embedded TPM v1.2 on the motherboard.
- Microsoft Windows Server software does not support trusted-boot scenarios that are supported by Intel TXT; use cases are based around Linux based server platforms which also includes VMWare ESXi and variations of Openstack cloud-server software.
- Trusted Boot (tboot) is an open source, pre- kernel/VMM module that uses Intel Trusted Execution Technology (Intel TXT) to perform a measured and verified launch of an OS kernel/VMM. Project details: http://sourceforge.net/projects/tboot/

Intel, the Intel logo, and Xeon, are trademarks of Intel Corporation in the U.S. and/or other countries. *Other names and brands may be claimed as the property of others. All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest Intel product specifications and roadmaps. Statements in this document that refer to Intel's plans and expectations for the quarter, the year, and the future, are forward-looking statements that involve a number of risks and uncertainties. A detailed discussion of the factors that could affect Intel's results and plans is included in Intel's SEC filings, including the annual report on Form 10-K. Any forecasts of goods and services needed for Intel's operations are provided for discussion purposes only. Intel will have no liability to make any purchase in connection with forecasts published in this document. Copies of documents which have an order number and are referenced in this document may be obtained by calling 1-800-548-4725 or visit www.intel.com/design/literature.htm.
© 2014 Intel Corporation

IBM Servers - X3650M4 and X3530M4

Note: Both of these IBM Server Platforms have very similar BIOS and configuration. There may be some slight differences between each model, but in general the operations that are shown for the X3650M4 will work on the X3530M4 model as well.



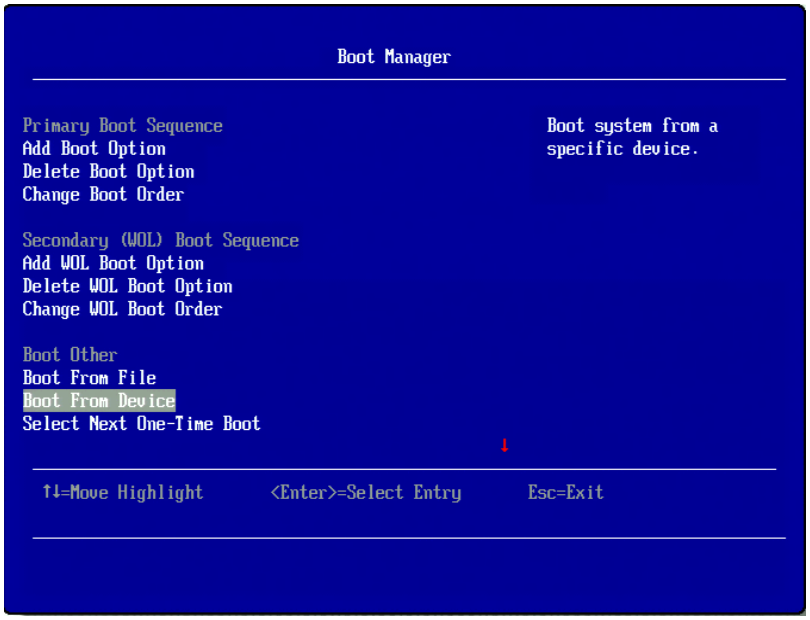
Platform Expectations

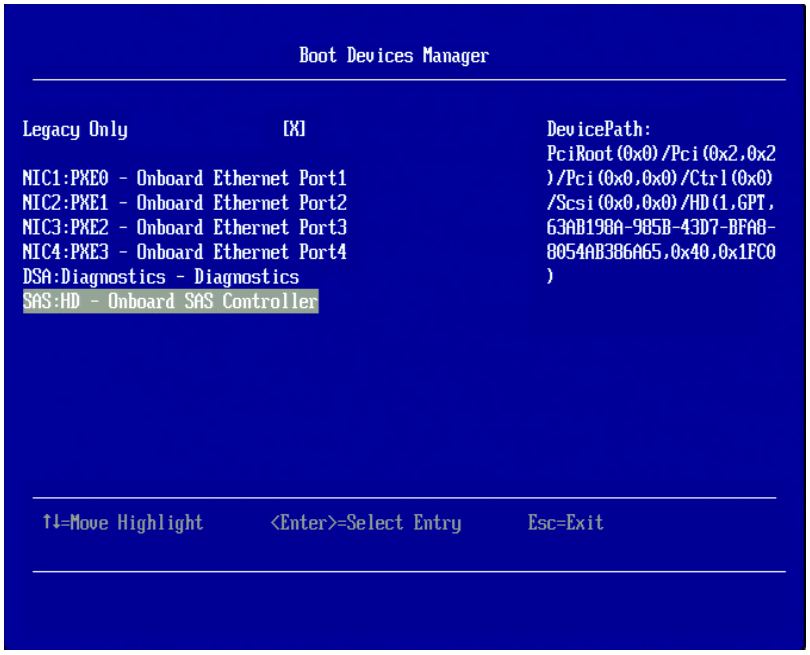
- IBM fully supports EFI and ships with native uEFI console
- IBM fully supports the TCG standard for Intel TXT/TPM activation which requires physical presence key
- IBM ships the TPM in enabled State by default.
- IBM ships the ACM as part of BIOS FW itself.

Out of the Box Configuration

1. By default IBM have TPM enabled
2. Press ***F1*** to enter to uEFI menu
3. Enter in to uEFI Menu ***> System Setting > System Security > TXT State > Enable***
4. Save Settings and Press ***Ctl+Alt+Del*** to reboot the server.
5. *Ensure to check if TPM Status is Enabled/Activated and Intel TXT status is enabled. Press F1>* ***System Setting > System Security***
6. ***uEFI Menu > Boot Manager > Boot from device > Legacy Only*** [*check/select*]; and select the boot device.. For ex: select CD ROM if user decides to install through CD medium

© Intel Corporation 2014





7. After Successful Installation, press *F1 > uEFI Menu > Boot Manager > Boot from device > legacy Only* [check/select] and select the boot device. For ex: On board SAS controller

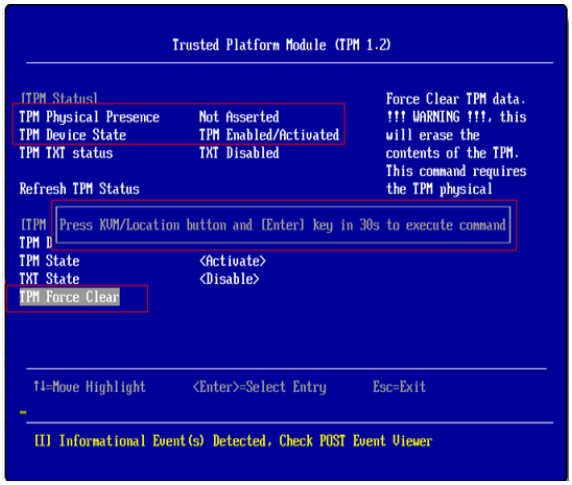
© Intel Corporation 2014

TPM Clear and Reactivate Intel TXT/TPM

After TPM clear action, IBM servers require ***physical presence button press*** to reactivate the TPM/Intel TXT.

TPM clear can be done either in BIOS console or from OS using Trousers DLL. One of the requirements for TPM clear is to transfer the TPM ownership. TPM clear action will deactivate the TPM. Reboot is required to activate the TPM/Intel TXT again. Below are the steps to clear and reactivate the TPM/Intel TXT.

- Press F1 > Systems Setting > System Security > Select "TPM Force Clear"
- User will get the prompt to press the KVM/Location Button next to power button in front panel.
- Press the KVM/Location button and hit Enter in 30 seconds.



- User will get a Success message. ***"Success! Reboot Required to enable this change"***
- Save the settings and reboot the server ***Ctl+Alt+Del***
- uEFI Menu > System Setting ***> System Security > TXT State > Enable***
- *Ensure to check if TPM Status is Enabled/Activated and Intel TXT status is* ***Enabled****.*
- uEFI Menu > Save Settings and Press ***Ctrl + del*** to Reboot the server.
- ***Press F1 > uEFI Menu > Boot Manager > Boot from device > Legacy Only*** [check/select] ; and select the boot device.. For ex: select CD ROM if user decides to install through CD medium
- **After Successful Installation**, ***press F1 > uEFI Menu > Boot Manager > Boot from device > legacy Only*** [check/select] and select the boot device. For ex: On board SAS controller

Note:

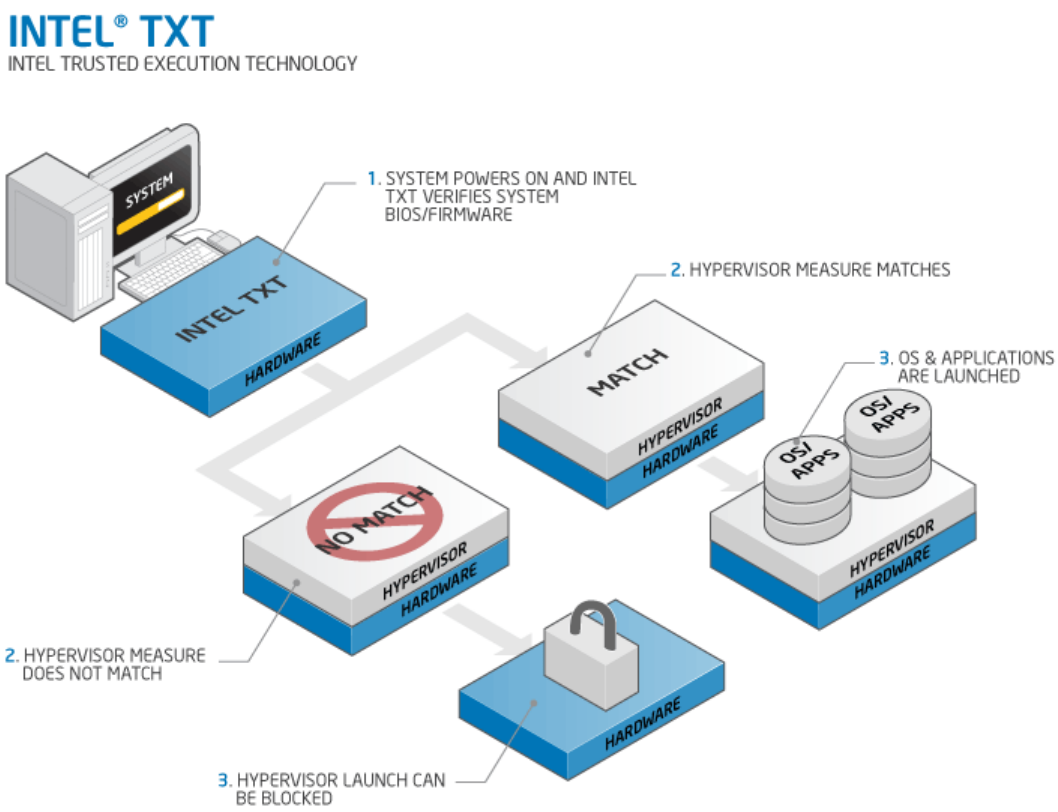
- All IBM servers have TPM enabled by default but Intel TXT is disabled.
- To Enable Intel TXT, user doesn't need to press KVM button.
- KVM button Press action needs only when user clears the TPM [ON/OFF].
- TPM ON and TPM activate can be done together and so KVM press actions is needed only one time for both ON and Activate actions.

Scaling Activation of Intel TXT/TPM across Multiple Systems

Enabling Intel TXT/TPM on one system is great for testing and validating your platform. In real-world scenarios in the datacenter, customers generally have multiple systems that need enabling at the same time during setup and configuration. Fortunately many OEMs provide tools that lend themselves to assist the server administrator to perform this function.

© Intel Corporation 2014

Enabling Intel TXT across multiple systems allows for more use cases beyond the root-of-trust establishment on a single platform. Models such as Trusted Compute Pools can be developed where systems with Intel TXT can be placed on a 'whitelist' for access. This allows system administrators to place their highest security workloads on trusted platforms and reduce the threat to bare-metal attacks.



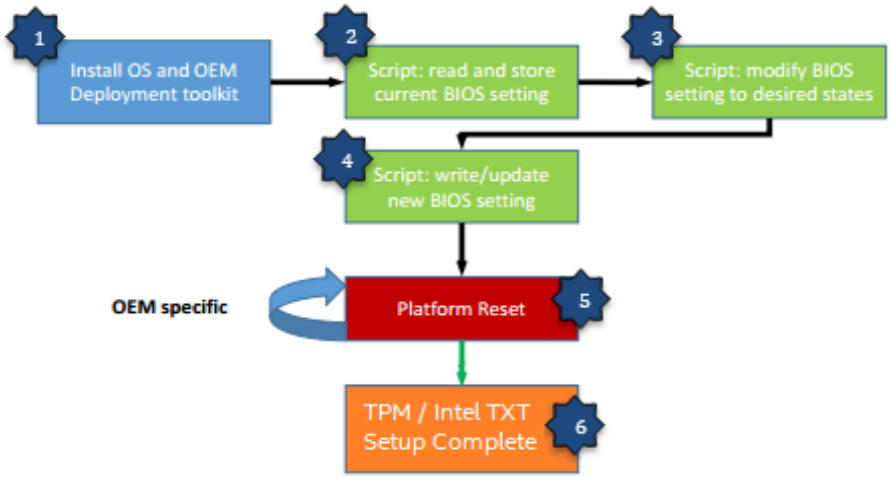
In order for Intel TXT to function properly the following dependencies need to be established:

- Intel Xeon processor based server platform with Intel TXT enabled BIOS
- 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 (TPM) v1.2 must be enabled and activated
- The platform specific Intel SINIT ACM needs to be installed into the platform
- Finally, you need a hypervisor that supports trusted boot (t-boot)

© Intel Corporation 2014

Bare Metal Provisioning of Intel TXT

The process to take a bare-metal system with unknown settings to a fully functional Intel TXT enabled platform can take a few minutes per system. The process can be run in-band from the OS, or out-of-band (OOB) via PXE or other remote process. The schematic below shows the high-level process of how a system is updated.



1. The Server PXE boots and installs the OS as well as the OEM deployment tool.
2. The setup and configuration script issues the command that reads the current BIOS setting of the server.
3. The setup and configuration script modifies the TPM/Intel TXT and other inter-related settings to the desired states as prescribed by the administrator.
4. The setup and configuration script issues command that writes and updates the BIOS setting then reboots the server.
5. After several reboots (OEM specific), the TPM/Intel TXT setting will take effect.
6. At this point, the server is automatically configured for TPM/Intel TXT support without accessing the BIOS manually.

Intel TXT Scale Provisioning for IBM Server Platforms

The IBM Advanced Settings Utility (ASU) can modify BIOS settings from the command line on multiple operating-system platforms. The ASU can perform the following tasks: modify the basic BIOS CMOS settings, Issue selected baseboard management controller setup commands, and issue selected Remote Supervisor Adapter and Remote Supervisor Adapter II (IMM2) setup commands.

The IBM ASU provides these benefits:

- Modify selected basic input/output system (BIOS) CMOS settings without the need to restart the system to access F1 settings
- Modify selected baseboard management controller setup settings
- Modify selected Remote Supervisor Adapter and Remote Supervisor Adapter II setup settings
- Secure boot configuration
- Mount ISO file or USB/CD/DVD to a remote IMM based system, IMM must be exposed to network and accessible

© Intel Corporation 2014

IBM ASU Installation

After downloading the IBM ASU, there are a few simple steps to deploy the ASU onto your system:

1. Open an xterm or other terminal window.
2. Go to the directory that contains the downloaded ASU files.
3. From a shell command prompt, type one of the following commands and press

- If the .tgz file for ASU was downloaded: Enter **tar -zxvf filename.tgz** where filename is the name of the Advanced Settings Utility file for Linux that you downloaded. The files are extracted to the same directory.
- If the .rpm file for ASU was downloaded: Enter **rpm -Uvh filename.rpm** where filename is the name of the Advanced Settings Utility file for Linux that you downloaded. The files are extracted to the */opt/ibm/toolscenter/asu directory*.

Here is an example of the configuration script that can be run on IBM Servers that will scan the BIOS, and change the appropriate settings that will set Intel TXT to be activated and ready for your hypervisor installation.

```
echo "read security current setting"
./asu64 show SystemSecurity --kcs
sleep 5

echo "read virtualization current setting"
./asu64 show Processor.IntelVirtualizationTechnology --kcs
sleep 5

echo "set virtualization setting"
./asu64 set Processor.IntelVirtualizationTechnology Enable --kcs
sleep 5

echo "set TXT setting"
./asu64 set SystemSecurity.TXTState Enable --kcs
sleep 5
```

How to check the Intel TXT/TPM status

Linux Distributions

Assumption:

- Users have successfully activated Intel TXT in BIOS and OS by following the respective guides.
- To Activate the Intel TXT in Linux OS users are requested to follow the Intel TXT OS Setup Guide.
- TPM Status Can be read from linux OS through TPM Device Driver in Dom0.
- Issue below command to find the status of the TPM

  $ cat /sys/class/misc/tpm0/device/enabled
  # If it returns 0 then it is not enabled; if it returns 1 then it is enabled.

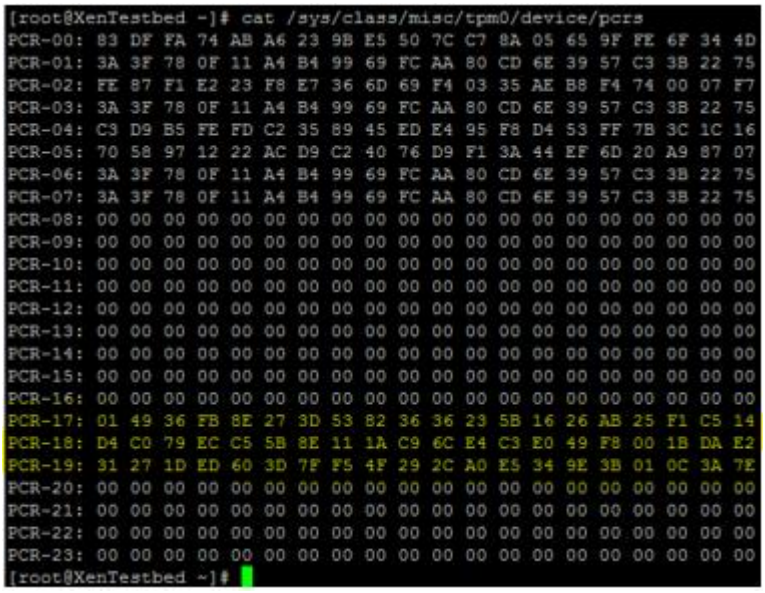
  $ cat /sys/class/misc/tpm0/device/active
  # If it returns o then it is not active; if it is returns 1 then it is active.

  $ cat /sys/class/misc/tpm0/device/owned

© Intel Corporation 2014

 # If it returns o then it is not owned; if it is returns 1 then it is owned.

$ cat /sys/class/misc/tpm0/device/pcrs
 # Returns the PCR measurement values.

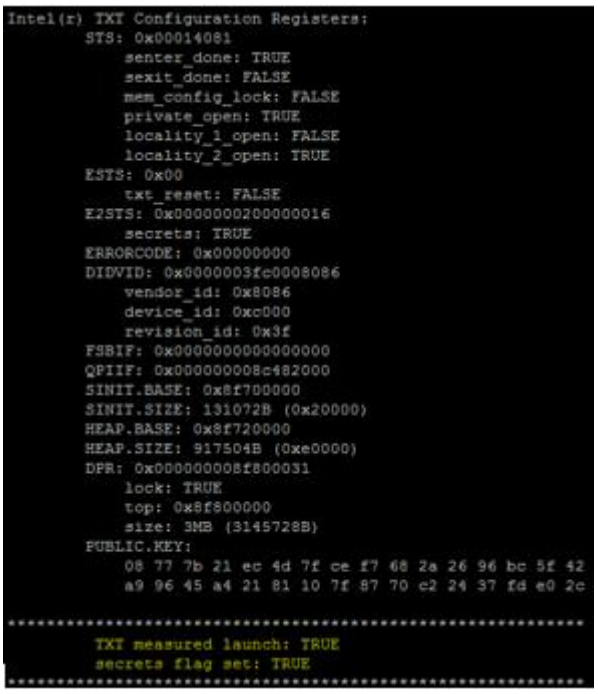


"Txt-stat" Tool:

- ***txt-stat*** is the Intel TXT status tool that is part of Tboot kernel to get the status of Intel TXT measurement.***txt-stat*** tool collects the information from RAM and displays.
- Users can use this tool to check if the Intel TXT launch/boot was successful or not.
- Ensure to run the **tcsd daemon** before running this tool.

$ tcsd
$ txt-stat | more

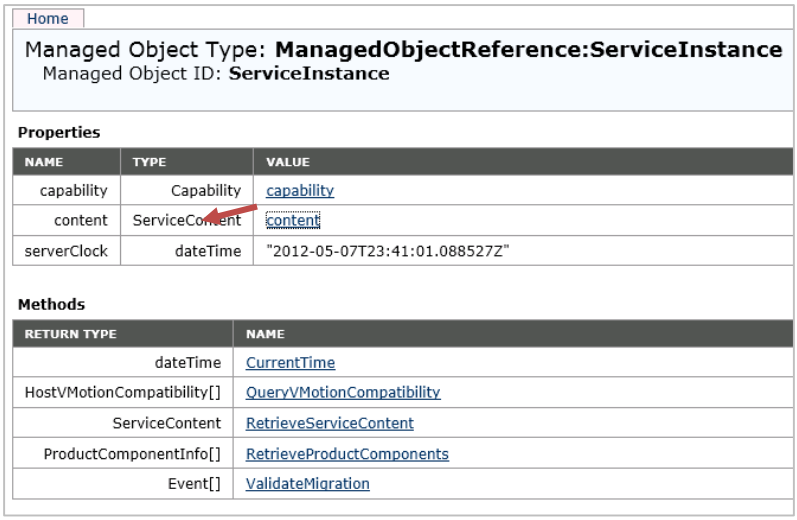
© Intel Corporation 2014



© Intel Corporation 2014

VMware ESXi 5.x

1. Install ESXi on the Intel TXT/TPM activated host and add to the vCenter.
2. Connect to the vCenter through IE browser *http://<vCenter IP Address>/mob*
3. Click on the "***add exceptions***" in the next screen
4. Enter the ***credentials*** of the vCenter to connect to ESXi hosts.
5. Click on "***Content***"



6. In the following screen, search for "***Rootfolder***" and click on the value "***group-d1***"
7. In the following screen, search for "***Childentity***" and click on the value "***Datacenter-2***"
8. In the following screen, search for "***Hostfolder***" and click on the value "***group-h4***"
9. In the following screen, search for "***Childentity***" and click on the value "***Domain-C7***"
10. In the following screen, search for "*Host*" and click on the value "***host <ip address>***"
11. In next screen drag down to Methods table and click on "***QueryTpmAttestationReport***"
12. A separate window will open up - Click on "***Invoke method***"
13. In the Next screen user can see the Platform Configuration Register (PCR) values populated.

Note:

- If *ESXi* host is not Intel TXT provisioned then you will not see any PCR values in step 13.
- If users are sure that TPM is provisioned correctly but TPM value is unset in v-center then as a work around, disconnects the host and reconnects the host if the TPM value is unset.

© Intel Corporation 2014

Troubleshooting Guide

1. **How to determine if Intel TXT successfully launched?**

   In Linux Distributions:
   Use txt-stat tool to check if the Intel TXT launch is successful.

```
root@ubuntu-tboot:~# txt-stat | grep measured
        TXT measured launch: TRUE
TBOOT: measured launch succeeded
```

   In VMware ESXi:
   You can verify if TPM is enabled on your ESXi hosts with the following command:
   esxcli hardware trustedboot get

```
~ # esxcli hardware trustedboot get
   Drtm Enabled: true
   Tpm Present: true
```

   If users see TPM value is unset though it is provisioned correctly, as a work around disconnect and reconnect the host in vCenter will usually resolve the issue.

2. **How to validate the TPM:**

   There is tool called tpm-tools which is shipped with all Linux OS. This tools implements the TSS API and talks directly to the TPM

   $ tpm_selftest will show the current state of TPM
   $ tpm_version will show the tpm version

```
root@mwtstubx01h:~# tpm_version
  TPM 1.2 Version Info:
  Chip Version:        1.2.8.8
  Spec Level:          2
  Errata Revision:     2
  TPM Vendor ID:       STM
  TPM Version:         01010000
  Manufacturer Info:   53544d20
```

© Intel Corporation 2014