

# TXT Provisioning Guide

OS: Ubuntu 11.10

VMM: XEN



IASI

CLOUD SOLUTIONS ENGINEERING

## Contents

<b>INTRODUCTION.....</b>	<b>5</b>
<b>SYSTEM HARDWARE REQUIREMENTS .....</b>	<b>5</b>
<b>SYSTEM SOFTWARE REQUIREMENTS .....</b>	<b>5</b>
<b>SECTION –I .....</b>	<b>5</b>
1.1 TXT/TPM Provisioning in BIOS setup.....	5
1.2 OS installation – Ubuntu 11.10 .....	6
1.3 OS configuration: .....	9
1.4 VMM Installation: .....	9
<b>SECTION -II .....</b>	<b>11</b>
1.1 Grub configuration/installation .....	11
1.2 GRUB File Modification .....	12
<b>SECTION -III .....</b>	<b>13</b>
1.1 Tboot installation.....	13
1.2 TCG software Stack installation .....	16
<b>SECTION –IV .....</b>	<b>16</b>
1.3 Trust Agent Prerequisites .....	16

<b>1.4</b>	<b>Trust Agent Installation/Configuration .....</b>	<b>Error! Bookmark not defined.</b>
------------	---	-------------------------------------

DRAFT

## INTEL CONFIDENTIAL

The information in this manual is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by Intel Corporation. Intel Corporation assumes no responsibility or liability for any errors or inaccuracies that may appear in this document or any software that may be provided in association with this document.

### Authors:

Kamal Natesan

Reviewers: Uttam Shetty, Raghu Yeluri, Bangalore Sudhir, Wheeler jerry

## Introduction

This document is intended to be used by Datacenter architects and developers designing solutions to extend the functionality of the Intel TXT. This document focuses on methodology and approaches with the step by step instructions to build the TXT test bed from linear perspective.

## System Hardware Requirements

Processor	Starting X5600 Processor codename: Westmere-EP
Chipset	Starting Intel® 5520 Chipset (codename: Tylersburg)
TPM Chip	v 1.1
RAM	Minimum 12 Gig
HDD	Minimum 60 Gig

## System Software Requirements

BIOS f/w	TXT Supported BIOS. Refer appendix for more detail on OEM bios
SINIT ACM	<a href="http://software.intel.com/en-us/articles/intel-trusted-execution-technology/">http://software.intel.com/en-us/articles/intel-trusted-execution-technology/</a>
Tboot file	<a href="http://sourceforge.net/projects/tboot/">http://sourceforge.net/projects/tboot/</a>
kvm	<a href="http://www.linux-kvm.org/page/Main_Page">http://www.linux-kvm.org/page/Main_Page</a>
TCG Software Stack	<a href="http://sourceforge.net/projects/trousers">http://sourceforge.net/projects/trousers</a>

## SECTION -I

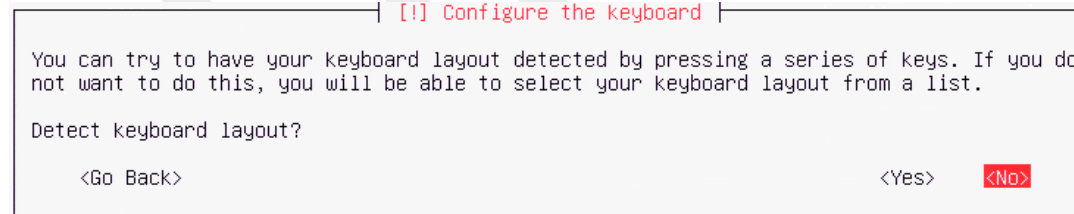
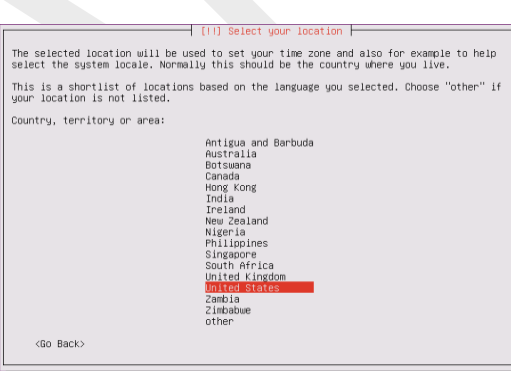
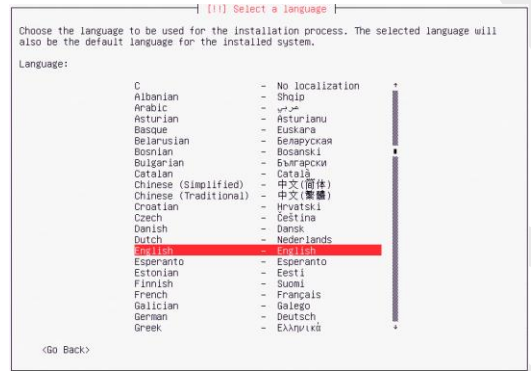
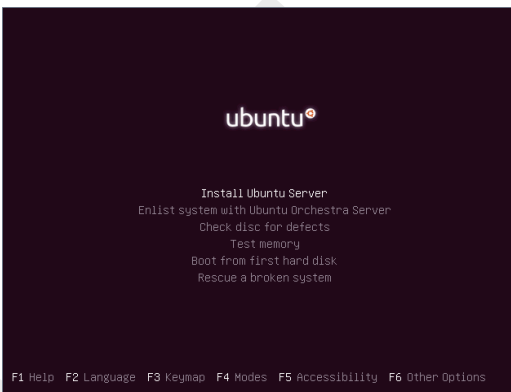
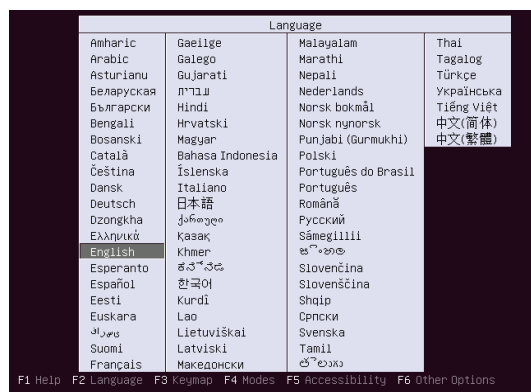
### 1.1 TXT/TPM Provisioning in BIOS setup

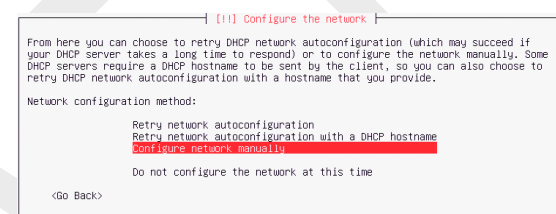
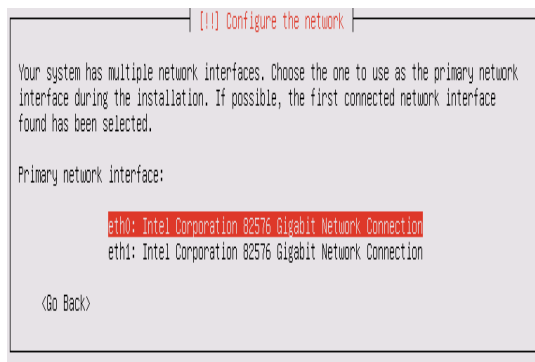
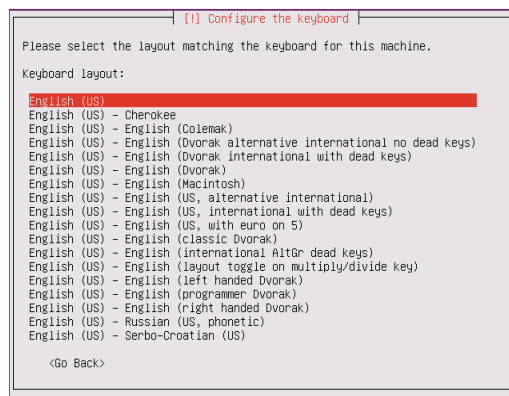
INTEL EPSD 1625UR	DELL Power Edge R710	HP DL380G7
Press F2 key to enter in to BIOS console	Press F2 key to enter in to BIOS console	Press F9 key to enter in to BIOS console
Setup BIOS password (Security > Set Administrator Password)	Setup BIOS password. (System Security > Password Status> locked) (System Security > System Password > Enabled) (System Security > Setup Password)	Set the BIOS password (System Security > Set Admin Password)
Press F10 key twice to reboot the server	Press ESC key twice and select "save changes and exit"	Enable TPM (System Security > Trusted Platform Module > TPM Functionality > Enabled )
On Boot, press F2 and enter the BIOS password	On Boot, press F2 and enter the BIOS password	Enable TXT (System Security > Intel TXT support > Enabled)
Ensure VT/VT-d is enabled (Advanced > Processor Configuration > Enable VT)	Enable TPM (System Security > TPM security > On with Pre-boot Measurement) (System Security > TPM activation> Activate)	Press ESC key twice and Press F10 to "save changes and exit" to reboot the server
Ensure VT-d is enabled (Advanced > Processor Configuration > Enable VT-d)	Press ESC key twice and select "save changes and exit"	
Enable TPM (Security > TPM Admin Control > Turn ON)	On Boot, press F2 and enter the BIOS password	
Enable TXT (Advanced > Processor Configuration > TXT)	Enable TXT (System Security > Intel TXT> Enabled)	
Press F10 key twice to save and reboot the server	Press ESC key twice and select "save changes and exit" to reboot the server	

## 1.2 OS installation - Ubuntu 11.10

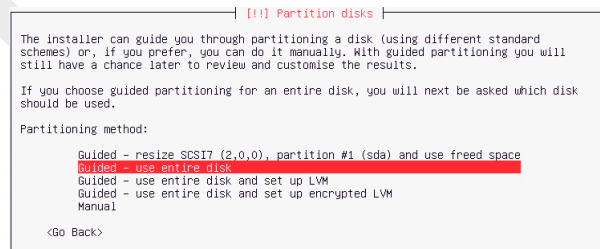
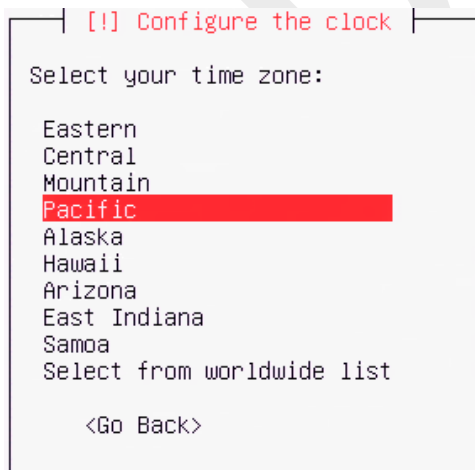
In this document we have covered the installation of Ubuntu 11.10 **Codename: oneiric** and **Kernel ver: 3.0.0-12-server**. Below steps will walkthrough OS installation/configuration with screenshot.

Step 1:





Note: Will be prompted to enter the network configuration



[!] Partition disks

Note that all data on the disk you select will be erased, but not before you have confirmed that you really want to make the changes.

Select disk to partition:

SCSI7 (2,0,0) (sda) - 146.0 GB INTEL SR08BSASMP2

<Go Back>

[!] Partition disks

If you continue, the changes listed below will be written to the disks. Otherwise, you will be able to make further changes manually.

WARNING: This will destroy all data on any partitions you have removed as well as on the partitions that are going to be formatted.

The partition tables of the following devices are changed:

SCSI7 (2,0,0) (sda)

The following partitions are going to be formatted:

partition #1 of SCSI7 (2,0,0) (sda) as ext4

partition #5 of SCSI7 (2,0,0) (sda) as swap

Write the changes to disks?

<Yes> <No>

[!] Set up users and passwords

A user account will be created for you to use instead of the root account for non-administrative activities.

Please enter the real name of this user. This information will be used for instance as default origin for emails sent by this user as well as any program which displays or uses the user's real name. Your full name is a reasonable choice.

Full name for the new user:

<Go Back> <Continue>

[!] Set up users and passwords

A good password will contain a mixture of letters, numbers and punctuation and should be changed at regular intervals.

Choose a password for the new user:

<Go Back> <Continue>

[!] Set up users and passwords

You may configure your home directory for encryption, such that any files stored there remain private even if your computer is stolen.

The system will seamlessly mount your encrypted home directory each time you login and automatically unmount when you log out of all active sessions.

Encrypt your home directory?

<Go Back> <Yes> <No>

[!] Configure the package manager

If you need to use a HTTP proxy to access the outside world, enter the proxy information here. Otherwise, leave this blank.

The proxy information should be given in the standard form of "http://[user][:pass]@host[:port]/".

HTTP proxy information (blank for none):

<Go Back> <Continue>

Note: Enter the proxy setting if needed.

[!] Configuring tasksel

Applying updates on a frequent basis is an important part of keeping your system secure.

By default, updates need to be applied manually using package management tools. Alternatively, you can choose to have this system automatically download and install security updates, or you can choose to manage this system over the web as part of a group of systems using Canonical's Landscape service.

How do you want to manage upgrades on this system?

No automatic updates

Install security updates automatically

Manage system with Landscape

[!] Software selection

At the moment, only the core of the system is installed. To tune the system to your needs, you can choose to install one or more of the following predefined collections of software.

Choose software to install:

☒ OpenSSH server  
☐ DNS server  
☐ LAMP server  
☐ Mail server  
☐ PostgreSQL database  
☐ Print server  
☐ Samba file server  
☐ Tomcat Java server  
☐ Virtual Machine host  
☐ Ubuntu desktop USB  
☐ Manual package selection

<Continue>

[!] Install the GRUB boot loader on a hard disk

It seems that this new installation is the only operating system on this computer. If so, it should be safe to install the GRUB boot loader to the master boot record of your first hard drive.

Warning: If the installer failed to detect another operating system that is present on your computer, modifying the master boot record will make that operating system temporarily unbootable, though GRUB can be manually configured later to boot it.

Install the GRUB boot loader to the master boot record?

<Go Back> <Yes> <No>



[!!!] Finish the installation

#### Installation complete

Installation is complete, so it is time to boot into your new system. Make sure to remove the installation media (CD-ROM, floppies), so that you boot into the new system rather than restarting the installation.

<Go Back>

<Continue>

Once the installation of the OS is complete, accept the prompt to reboot the computer.

### 1.3 OS configuration:

1. Login as user

```
administrator@ubuntu01:~$ sudo su -  
[sudo] password for administrator:  
root@ubuntu01:~#
```

2. Remove the "!" from the file "/etc/shadow"

```
root@ubuntu01:~# cat /etc/shadow  
root:!:15358:0:99999:7:::  
daemon:!:15358:0:99999:7:::  
bin:!:15358:0:99999:7:::  
sys:!:15358:0:99999:7:::  
sync:!:15358:0:99999:7:::  
games:!:15358:0:99999:7:::  
man:!:15358:0:99999:7:::  
lp:!:15358:0:99999:7:::  
mail:!:15358:0:99999:7:::  
news:!:15358:0:99999:7:::  
uucp:!:15358:0:99999:7:::  
proxy:!:15358:0:99999:7:::  
www-data:!:15358:0:99999:7:::
```

Remove the "!" from the file "/etc/shadow"

3. Enable Root user and set the Root password:

```
$ sudo passwd root
```

```
root@ubuntu01:~# passwd root  
Enter new UNIX password:  
Retype new UNIX password:  
passwd: password updated successfully  
root@ubuntu01:~#
```

### 1.4 VMM Installation:

1. Install the Xen hypervisor

```
$ apt-get install xen-hypervisor-4.1-amd64  
$ apt-get install xenwatch  
$ apt-get install xen-utils-common  
$ apt-get install xenstore-utils  
$ apt-get install xen-utils-4.1  
$ apt-get install gcc-multilib xz-utils  
$ apt-get install bcc  
$ apt-get install virtinst virt-viewer virt-manager
```

## 2. Verify that Xen is running correctly

```
$ xl list
```

```
root@mwtstubx01h:~# xl list
Name                               ID   Mem VCPUs   State   Time(s)
Domain-0                           0  1024    1   r-----   34.8
```

```
$ xm info | more
```

```
root@mwtstubx01h:~# xm info | more
host                               : mwtstubx01h
release                           : 3.0.0-12-server
version                           : #20-Ubuntu SMP Fri Oct 7 16:36:30 UTC 2011
machine                           : x86_64
nr_cpus                           : 24
nr_nodes                          : 2
cores_per_socket                  : 6
threads_per_core                  : 2
cpu_mhz                           : 3325
hw_caps                           : bfebfbff:2c100800:00000000:00003f40:029ee3ff:00000000:0
0000001:00000000
virt_caps                         : hvm hvm_directio
total_memory                      : 12222
free_memory                       : 11028
free_cpus                         : 0
xen_major                         : 4
xen_minor                        : 1
xen_extra                         : .1
xen_caps                          : xen-3.0-x86_64 xen-3.0-x86_32p hvm-3.0-x86_32 hvm-3.0-x
86_32p hvm-3.0-x86_64
xen_scheduler                     : credit
xen_pagesize                      : 4096
platform_params                   : virt_start=0xffff800000000000
```

## 3. Configure the installation of XEN by edit the xend-config.sxp. Backup your xend-config.sxp before make changes to the xend-config.sxp

```
root@mwtstubx01h:/etc/xen# cp xend-config.sxp xend-config.sxp.old
```

Edit the /etc/xen/xend-config.sxp file with below info:

```
$ vi /etc/xen/xend-config.sxp
```

i) Remove the comment

```
(logfile /var/log/xen/xend.log)
(loglevel DEBUG)
```

ii) Remove the comment for XEN API settings and set to yes

```
(xend-unix-server yes)
```

iii) Add Network bridge and virtual interface scripts to xend.config.sxp and Save

```
(network-script network-bridge netdev=eth0)
(network-script /bin/true)
```

Edit your .bashrc file and add the line below. Save the file and then reboot

```
root@mwtstubx01h:~# cd /root
root@mwtstubx01h:~# vi .bashrc
export VIRSH_DEFAULT_CONNECT_URI="xen://"
```

After rebooted the server, confirm if you can connect to your Xen server using virsh command

```
root@mwtstubx01h:~# virsh version
Compiled against library: libvir 0.9.2
Using library: libvir 0.9.2
Using API: Xen 3.0.1
Running hypervisor: Xen 4.1.0
```

## SECTION -II

### 1.1 Grub configuration/installation

By default Ubuntu 11.10 installs the “grub2” boot loader. “GRUB2” will boot directly to the login prompt or Desktop. No menu will be displayed and there is no /boot/grub/menu.lst file. In order to edit the grub file, the user will need to downgrade from the default “grub2” to the older “grub” boot loader.

Perform the following steps to uninstall “grub2” and install “grub.”

1. Login as root user, and copy the existing grub folder to a backup.

```
$ cp /etc/default/grub /etc/default/grub.old
$ cp -R /etc/grub.d /etc/grub.d.old
$ cp -R /boot/grub /boot/grub.old
```

2. Remove the “grub2” boot loader

```
$ apt-get purge grub2 grub-pc
▪ Tab to “yes” when prompted
```

3. Install the downgraded “grub” boot loader

```
$ apt-get install grub
```

4. Determine the mount point of the boot loader

```
$ mount
```

```
administrator@ubuntu01:/boot/grub$ mount
/dev/sda1 on / type ext4 (rw,errors=remount-ro)
proc on /proc type proc (rw,noexec,nosuid,nodev)
sysfs on /sys type sysfs (rw,noexec,nosuid,nodev)
fusectl on /sys/fs/fuse/connections type fusectl (rw)
none on /sys/kernel/debug type debugfs (rw)
none on /sys/kernel/security type securityfs (rw)
udev on /dev type devtmpfs (rw,mode=0755)
devpts on /dev/pts type devpts (rw,noexec,nosuid,gid=5,mode=0620)
tmpfs on /run type tmpfs (rw,noexec,nosuid,size=10%,mode=0755)
none on /run/lock type tmpfs (rw,noexec,nosuid,nodev,size=5242880)
none on /run/shm type tmpfs (rw,nosuid,nodev)
administrator@ubuntu01:/boot/grub$
```

5. Write the “grub” boot loader to the appropriate mount point

```
$ grub-install /dev/sda
```

Choose the correct device as marked in above snapshot.  
Ensure it creates the stage1 & stage2 files in /boot/grub and writes to the MBR.

```
root@mwststubb01h:~# grub-install /dev/sda1
Searching for GRUB installation directory ... found: /boot/grub
Installing GRUB to /dev/sda1 as (hd0,0)...
Installation finished. No error reported.
This is the contents of the device map /boot/grub/device.map.
Check if this is correct or not. If any of the lines is incorrect,
fix it and re-run the script `grub-install'.

(fd0)    /dev/fd0
(hd0)    /dev/sda
```

6. Run the “update-grub” command to generate the “menu.lst” file

```
$ update-grub
  ▪ Tab to “yes” when prompted
```

7. Reboot the server

```
$ reboot
```

## 1.2 GRUB File Modification

- 1) Edit the new grub file “/boot/grub/menu.lst” as shown in the below screenshots

```
$ vim /boot/grub/menu.lst
```

By default, the menu.lst file will look like this:

```
## ## End Default Options ##

title          Ubuntu 11.10, kernel 3.0.0-12-server
uuid           9b19713b-fac3-4232-98b9-09d988960eac
kernel         /boot/vmlinuz-3.0.0-12-server root=UUID=9b19713b-fac3-4232-98b9-09d988960eac ro quiet splash
initrd         /boot/initrd.img-3.0.0-12-server
quiet

title          Ubuntu 11.10, kernel 3.0.0-12-server (recovery mode)
uuid           9b19713b-fac3-4232-98b9-09d988960eac
kernel         /boot/vmlinuz-3.0.0-12-server root=UUID=9b19713b-fac3-4232-98b9-09d988960eac ro single
initrd         /boot/initrd.img-3.0.0-12-server

title          Ubuntu 11.10, memtest86+
uuid           9b19713b-fac3-4232-98b9-09d988960eac
kernel         /boot/memtest86+.bin
quiet
```

- 2) Change the timeout to > 5

```
# You can specify 'saved' instead of a number. In this case, the default entry
# is the entry saved with the command 'savedefault'.
# WARNING: If you are using dmraid do not use 'savedefault' or your
# array will desync and will not let you boot your system.
default      0

## timeout sec
# Set a timeout, in SEC seconds, before automatically booting the default entry
# (normally the first entry defined).
timeout      10
```

- 3) Save and Reboot the server to verify that the changes are being reflected.

```
$ reboot
```

## SECTION -III

### 1.1 Tboot installation

1. Login as root user and install tboot.


```
$ apt-get install tboot
```

```
root@ubuntu01:~# apt-get install tboot
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  libtspi1
The following NEW packages will be installed:
  libtspi1 tboot
0 upgraded, 2 newly installed, 0 to remove and 50 not upgraded.
Need to get 479 kB of archives.
After this operation, 1,241 kB of additional disk space will be used.
Do you want to continue [Y/n]? y
Get:1 http://us.archive.ubuntu.com/ubuntu/ oneiric/main libtspi1 amd64 0.3.5-4 [178 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu/ oneiric/universe tboot amd64 1.6-0ubuntu1 [301 kB]
Fetched 479 kB in 1s (274 kB/s)
Selecting previously deselected package libtspi1.
(Reading database ... 49723 files and directories currently installed.)
Unpacking libtspi1 (from .../libtspi1_0.3.5-4_amd64.deb) ...
Selecting previously deselected package tboot.
Unpacking tboot (from .../tboot_1.6-0ubuntu1_amd64.deb) ...
Setting up libtspi1 (0.3.5-4) ...
Setting up tboot (1.6-0ubuntu1) ...
Processing triggers for libc-bin ...
ldconfig deferred processing now taking place
root@ubuntu01:~# cd /boot/
root@ubuntu01:/boot# ll
total 21900
drwxr-xr-x  3 root root    4096 2012-01-19 03:27 ./
drwxr-xr-x 23 root root    4096 2012-01-19 02:28 ../
-rw-r--r--  1 root root 730753 2011-10-07 16:58 abi-3.0.0-12-server
-rw-r--r--  1 root root 134862 2011-10-07 16:58 config-3.0.0-12-server
drwxr-xr-x  3 root root   12288 2012-01-19 03:26 grub/
-rw-r--r--  1 root root 13643049 2012-01-19 02:33 initrd.img-3.0.0-12-server
-rw-r--r--  1 root root 176764 2011-05-02 19:07 mentest86+.bin
-rw-r--r--  1 root root 178944 2011-05-02 19:07 mentest86+_multiboot.bin
-rw-r--r--  1 root root 2719829 2011-10-07 16:58 System.map-3.0.0-12-server
-rw-r--r--  1 root root 73099 2011-08-26 16:41 tboot.gz
-rw-r--r--  1 root root 8799 2011-08-26 16:41 tboot-syms
-rw-r--r--  1 root root 1366 2011-10-07 17:04 uncoreinfo-3.0.0-12-server
-rw-r--r--  1 root root 4718160 2011-10-07 16:58 unlinux-3.0.0-12-server
root@ubuntu01:/boot#
```

*Note: Tboot.gz will be loaded in /boot*

2. Copy the SINIT ACM from below link.  
<http://software.intel.com/en-us/articles/intel-trusted-execution-technology/>

Server Platform	CPU	Chipset	ID	SINIT AC Filename	Kit Download
(codename: Thurley/Tylersburg)	Intel® Xeon® Processor 5600 Series and 3500 Series (codenames: Westmere-EP and Westmere-W)	Intel® 5520, 5500, and X58 Chipsets (codename: Tylersburg)	TXT.DIDVID.DeviceID: 0x3406h	Xeon-5600-3500-SINIT_v1.1.BIN	Xeon-5600-3500- SINIT_v1.1.zip

3. Extract the .bin file from the .zip archive  
 37,120 BIN File
4. Copy the .bin file into the /boot directory

Note: For Romley Based servers the SINIT ACM is part of BIOS itself. So above steps 2 and 3 is not required for Intel E5xxx based processors.

5. Modify the menu.lst file to add an additional boot option as per below snapshot

```
$ vim /boot/grub/menu.lst
```

```
title      Xen 4.1-amd64 / Ubuntu 11.10, kernel 3.0.0-12-server Tboot/TXT
#uuid     37fa36f3-65e3-4dcc-alb7-0bleffd7ef2d
kernel    /boot/tboot.gz logging=memory
module    /boot/xen-4.1-amd64.gz dom0_mem=1024M cpufreq=xen dom0_max_vcpus=1 dom0_vcpus_pin
module    /boot/vmlinuz-3.0.0-12-server root=/dev/sda1 ro console=tty0
module    /boot/initrd.img-3.0.0-12-server
module    /boot/Xeon-5600-3500-SINIT-v1.1.bin
```

The entire section should look like this:

```
## ## End Default Options ##

title      Xen 4.1-amd64 / Ubuntu 11.10, kernel 3.0.0-12-server Tboot/TXT
#uuid     37fa36f3-65e3-4dcc-alb7-0bleffd7ef2d
kernel    /boot/tboot.gz logging=memory
module    /boot/xen-4.1-amd64.gz dom0_mem=1024M cpufreq=xen dom0_max_vcpus=1 dom0_vcpus_pin
module    /boot/vmlinuz-3.0.0-12-server root=/dev/sda1 ro console=tty0
module    /boot/initrd.img-3.0.0-12-server
module    /boot/Xeon-5600-3500-SINIT-v1.1.bin

title      Ubuntu 11.10, kernel 3.0.0-12-server
uuid      37fa36f3-65e3-4dcc-alb7-0bleffd7ef2d
kernel    /boot/vmlinuz-3.0.0-12-server root=UUID=37fa36f3-65e3-4dcc-alb7-0bleffd7ef2d ro qui
et splash
initrd    /boot/initrd.img-3.0.0-12-server
quiet

title      Ubuntu 11.10, kernel 3.0.0-12-server (recovery mode)
uuid      37fa36f3-65e3-4dcc-alb7-0bleffd7ef2d
kernel    /boot/vmlinuz-3.0.0-12-server root=UUID=37fa36f3-65e3-4dcc-alb7-0bleffd7ef2d ro si
ngle
initrd    /boot/initrd.img-3.0.0-12-server

title      Ubuntu 11.10, memtest86+
uuid      37fa36f3-65e3-4dcc-alb7-0bleffd7ef2d
kernel    /boot/memtest86+.bin
quiet
```

6. Reboot the server and login as root user.

```
$ reboot
```

7. Upon rebooting, a boot menu will be displayed allowing the user to select which environment to boot to. Select the first option to boot with TXT/tboot.

```
Xen 4.1-amd64 / Ubuntu 11.10, kernel 3.0.0-12-server Tboot/TXT
Ubuntu 11.10, kernel 3.0.0-12-server
Ubuntu 11.10, kernel 3.0.0-12-server (recovery mode)
Ubuntu 11.10, memtest86+
```

Use the ↑ and ↓ keys to select which entry is highlighted.  
Press enter to boot the selected OS, 'e' to edit the  
commands before booting, or 'c' for a command-line.

The highlighted entry will be booted automatically in 6 seconds.

8. PCR 17-19 should now appear populated when queried using the below command:

```
$ cat /sys/class/misc/tpm0/device/pcrs
```

```
root@mwststux01h:/# cat /sys/class/misc/tpm0/device/pcrs
PCR-00: 89 1E B0 B5 56 B8 3F CE F1 C1 0F 3F A6 46 43 45 E3 4F 8F 91
PCR-01: 3A 3F 78 0F 11 A4 B4 99 69 FC AA 80 CD 6E 39 57 C3 3B 22 75
PCR-02: AE 8E 00 D7 A3 56 CB 8A 34 56 E8 36 68 84 69 FB 04 69 96 65
PCR-03: 3A 3F 78 0F 11 A4 B4 99 69 FC AA 80 CD 6E 39 57 C3 3B 22 75
PCR-04: 77 63 05 E6 09 8A DF C3 D8 92 DF 07 E1 37 12 39 06 BA 51 89
PCR-05: 42 99 B4 AE 29 4E 72 29 AB 62 F3 55 DB 89 19 3F 58 76 A6 F9
PCR-06: 3A 3F 78 0F 11 A4 B4 99 69 FC AA 80 CD 6E 39 57 C3 3B 22 75
PCR-07: 3A 3F 78 0F 11 A4 B4 99 69 FC AA 80 CD 6E 39 57 C3 3B 22 75
PCR-08: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR-09: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR-10: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR-11: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR-12: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR-13: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR-14: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR-15: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR-16: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR-17: BF C3 FF D7 94 0E 92 81 A3 EB FD FA 4E 04 12 86 9A 3F 55 D8
PCR-18: A7 13 C5 3F D7 D6 84 F0 C6 35 43 2B BE EF F6 23 5C ED 4E C3
PCR-19: E2 72 4C 0C DD EB 0D DF E8 75 A8 F3 A1 5F 8A F2 5F A0 13 96
PCR-20: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR-21: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR-22: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
PCR-23: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

## TCG software Stack installation

1. Login as root user and install trousers

```
$ apt-get install trousers
```

ii	Name	Version	Description
ii	trousers	0.3.5-4	open-source TCG Software Stack (daemon)

```
$ apt-get install trousers-dbg
```

ii	Name	Version	Description
ii	trousers-dbg	0.3.5-4	open-source TCG Software Stack (debug)

2. Run the TCSD daemon in the background.

```
$ tcsd
```

## SECTION -IV

### 1.2 Trust Agent Prerequisites

1. Install the remaining software prerequisites

```
$ apt-get install curl  
$ apt-get install libcurl3-openssl-dev  
$ apt-get install chkconfig  
$ apt-get -f install  
$ apt-get install make
```