Step-by-Step Configuration Guide: Trusted Compute Pools in Red Hat Enterprise Linux* OpenStack* Platform

Table of Contents

1 Introduction. 2

2 Deployment Environment 3

3 Provisioning and Configuration Recommendations 3

3.1 Switch Configuration. 4

3.2 Provisioning – Cobbler 4

3.3 Configuration Management – Puppet 4

4 Intel® Trusted Execution Technology. 5

4.1 Initial Installation. 5

4.2 Changes to the MLE: Kernel, BIOS, Module Upgrades, Grub Boot Options 6

5 OpenAttestation. 7

5.1 OpenAttestation Server Installation 7

5.1.1 Enable epel/epel-oat/rhn base/rhn Optional Repositories 7

5.1.2 Installation. 7

5.2 OpenAttestation Client Installation. 8

5.3 Node Whitelisting 8

5.2.1 Initial Installation 8

5.2.2 System Maintenance and Upgrades. 8

6 OpenStack Configuration 8

7 Creating Trusted Instances with the Horizon Dashboard 10

8 Conclusion 10

Resources. 11

This document outlines a specific step-by-step installation and configuration of Trusted Compute Pools with the Red Hat Enterprise Linux OpenStack Platform.

Dan Yocum, Red Hat, Inc.   **Matt Woodson,** Red Hat, Inc.   **Gang (Jimmy) Wei,** Intel Corporation

1 Introduction

Enterprise IT organizations and cloud service providers are increasingly attracted to open-source cloud platforms, which offer advantages that include low cost, flexible licensing, vendor choice, and the high degree of innovation that the open-source community provides. Zenoss Inc. reported that 56.9 percent of IT professionals responding to a survey are considering deployment of an open-source cloud and that their dominant platform of choice is OpenStack*.[1]

At the same time, IDC and IDG reported that 70 percent of survey respondents identified concerns about security as one of their top three challenges or obstacles to implementing cloud computing solutions. In overcoming those concerns and enabling the hosting of all workloads, including those that depend on sensitive information, robust security mechanisms play a vital role.[2]

Intel and Red Hat have collaborated closely to enable those mechanisms in Red Hat Enterprise Linux* OpenStack Platform running on Intel® architecture. Clouds based on this solution stack take advantage of a combination of hardware-based and software-based mechanisms to help ensure that cloud-based execution environments remain free of intrusion or tampering.

The key components of this open-source approach include the following:

- **Red Hat Enterprise Linux OpenStack Platform** applies Red Hat's open-source software expertise to the highly scalable OpenStack cloud computing platform. It helps customers reduce complexity and confidently adopt an enterprise-ready OpenStack distribution, with rapid access to bug fixes and security patches, plus tight integration with Red Hat's enterprise security features, including SELinux*.
- **Intel® Trusted Execution Technology** (Intel® TXT),[3] a hardware-based feature of many systems based on the Intel® Xeon® processor, compares the launch environment's BIOS, OS, and hypervisor at boot time to the expected "known good" boot environment to verify that the environment has not been tampered with and can thus be considered a "trusted platform."

NOTE: Trusted Boot (tboot) is the open-source project that delivers Intel TXT support into the hypervisor or OS.

- **OpenAttestation** is an installable service, available through open source, that retrieves verification data generated by Intel TXT on remote hosts to centralized cloud-management software, to provide a cloud-wide view of the integrity of all hosts and provide attestable hardware support for auditing and compliance requirements.
- **Trusted Compute Pools** are the groups of platforms verified using mechanisms based on Intel TXT and OpenAttestation as being intact and thus free of malware and other tampering at boot time; these platforms are considered trusted for hosting privileged or sensitive data and workloads.
- **OpenStack Nova scheduler** compares key/value pairs returned by OpenAttestation to expected values using filters that identify trusted hosts, which are candidates for the scheduler to place VMs for workload execution.

This document provides background and step-by-step procedures for installing and configuring the hardware and software that underlie these capabilities. It was developed using the OnRamp/TestFlight environment, which was built by Intel and Red Hat to showcase Intel TXT, OpenAttestation, and Red Hat Enterprise Linux OpenStack Platform.

This configuration guide is written based on the following assumptions:

- Red Hat Enterprise Linux has been freshly installed.
- A Trusted Platform Module (TPM)—a hardware-based key storage and retrieval component whose technical specification was written by a computer industry consortium called the Trusted Computing Group (TCG)—is installed on the motherboard.
- Network connectivity is available.
- Red Hat Enterprise Linux 6.5 is being used.
- OpenAttestation 1.6.0 is being used.

2 Deployment Environment

This document was prepared using the hardware and software components listed in Table 1.

NOTE: Deployment procedures for upgrading the TestFlight environment to the latest Icehouse release are in the process of being developed and tested.

Table 1. Components of the deployment environment.

OpenStack* Control and Compute Nodes	Dell PowerEdge* R620 servers: • Dual Intel® Xeon® processors E5-2620 (six cores per socket) • 132 GB RAM • 300 GB of RAID 1 disk • Dual Intel® Ethernet Converged Network Adapters X540
OpenStack Storage Nodes (Cinder and Swift Servers)	Dell PowerEdge R720 servers: • Dual Intel Xeon processors E5-2670 (eight cores per socket) • 132 GB RAM • 3.5 TB of RAID 10 disk • Dual Intel Ethernet Converged Network Adapters X540
Switch: Intra-Cloud Communication	Dell Force10* S4810
Switch: Management and External Connectivity	Dell PC5548
Software	Red Hat Enterprise Linux OpenStack Platform 3 (Grizzly) OpenAttestation 1.6.0 Red Hat Enterprise Linux 6.5

3 Provisioning and Configuration Recommendations

The recommendations in this section are based on problem resolutions and other findings during the testing performed for the preparation of this document.

3.1 Switch Configuration

Enabling Bridge Protocol Data Unit Guard (bpduguard) on intra-cloud communication switch ports (the Dell Force10 switch in this configuration) can interfere with network traffic.

When a port configured with bpduguard receives a BPDU STP frame from another switch, it shuts down until the STP frames cease. Because Linux network bridge interfaces, by default, enable STP frames and emit BPDU frames, ports placed—for example—into mode "spanning-tree rstp edge-port bpduguard" will cause ports on the intra-cloud communication switch to shut down.

The simplest recommendation in this area is to not enable bpduguard (it is disabled by default on Dell Force10 switches). Alternatively, the following line can be added to the /etc/sysconfig/ifcfg-brN files on the host node:

```
STP=no
```

3.2 Provisioning – Cobbler

While deploying Cobbler is outside the scope of this document, this section describes specific differences among the various types of OpenStack nodes used in the TestFlight cloud.

Environments based on the Red Hat Enterprise Linux OpenStack Platform must be designed correctly to avoid creating single points of failure. Because most OpenStack services have been designed with horizontal scalability explicitly in mind, placing a load balancer in front of all services further reduces the chances of client-accessible component failure. TestFlight has been deployed in such a configuration.

The TestFlight cloud requires six types of systems for basic operation; each has distinct system requirements, necessitating a separate kickstart file for each. The following is a list of the systems and their different kickstart installation parameters.

- **OpenStack Controller node**. The node must be installed on bare metal to enable access to the TPM for Intel TXT, specifically to gain query access to the OpenAttestation service.
- **OpenStack Compute node**
  - o The node must be installed on bare metal to access the TPM for Intel TXT, specifically to launch the trusted virtual machine (VM) image flavor.
  - o The size of /var should be 20 GB to accommodate snapshotting VMs.
  - o Swap should be as large as the memory overcommit has been set to; for example, if memory overcommit is set to 3x the physical RAM of 128 GB, swap should be ~375 GB.
- **OpenStack Cinder node**. The node should be installed on bare metal for optimum disk I/O performance.
- **MySQL* server**
  - o The node can be installed on a VM.
  - o The size of /var should be 20 GB.
- **Qpid server**. The node can be installed on a VM.
- **HA load balancer (LVS)**. The node can be installed on a VM.
- **OpenStack Swift server (optional)**. The node should be installed on bare metal for optimum disk I/O performance.

3.3 Configuration Management – Puppet

While deploying Puppet is outside the scope of this document, an automated configuration management system such as Puppet is recommended for managing the large number of services and configuration files hosted on various nodes.

As a base for installing and configuring the OpenStack services, following the recommended best practices for Red Hat Enterprise Linux OpenStack Platform, TestFlight has been deployed using the StackForge modules hosted at github: https://github.com/stackforge.

4 Intel® Trusted Execution Technology

To provide a Trusted Boot environment, Intel TXT verifies the following as known good, trusted versions when a system is booted:

- BIOS image
- Kernel images
- All modules loaded at boot time
- All grub boot options (verifying that they have been set by a trusted system administrator)

These items comprise the Measured Launch Environment (MLE). Intel TXT creates a checksum of these items, hashes the checksums together, signs them with a cryptographic key, and writes the resulting value to the TPM.

During a system boot or reset, each component is measured by the tboot environment and compared against the known good values stored in the TPM. If the hash of the measured components matches what is in the TPM, everything is deemed to be trusted and the system continues to boot. If the hash of the measured components does NOT match, a Launch Control Policy (LCP) either causes the system to refuse to boot, or, if the system is allowed to boot, to not be placed in the trusted pool of systems using the OpenAttestation service.

NOTE: Mechanisms based on Intel TXT do not continue to ensure a trusted and secure environment after the system is booted, such as if a rootkit is installed or malware is executed. While the use of SELinux is recommended to ensure that a system maintains its integrity while in operation, that implementation is outside the scope of this document.

4.1 Initial Installation

The general workflow to enable Intel TXT is as follows:

1. To enable the TPM, enter the BIOS during POST and make the following settings (examples based on a Dell PowerEdge R620 server):

Virtualization (VT-d)	Enabled (default)
TPM Security	On with Pre-boot Measurement
TPM Activation	No Change
TPM Status	Enabled, Activated
TPM Clear	No
Intel TXT	ON

2. After booting into Red Hat Enterprise Linux v6.5 and registering the system with RHN or RHN Classic, install **tboot** and **tpm-tools**, and enable the **tcsd** service:

```
$ yum -y install tboot tpm-tools
$ chkconfig tcsd on
```

Download automation scripts for lcp/tb policy setup from txt-oat repo:

NOTE: These scripts will be added into tboot RPM later.

```
$ mkdir ~/bin; cd ~/bin
$ wget  https://github.com/yocum137/txt-oat/
raw/master/scripts/create-lcp-tboot-policy.sh
$ wget https://github.com/yocum137/txt-oat/
raw/master/scripts/update-tboot-policy.sh
$ chmod 750 create-lcp-tboot-policy.sh
update-tboot-policy.sh
```

3. Configure the first boot entry in **grub.conf** as follows (note that **list.data** is commented out):

```
title Secure Red Hat Enterprise Linux Server
(2.6.32-431.5.1.el6.x86_64)
  root (hd0,0)
  kernel /tboot.gz logging=vga,serial,memory
  module /vmlinuz-2.6.32-431.5.1.el6.x86_64 ro
    root=/dev/mapper/VolGroup-lv_root intel_
    iommu=on rd_NO_LUKS
    LANG=en_US.UTF-8 rd_NO_MD rd_LVM_
    LV=VolGroup/lv_swap
    SYSFONT=latarcyrheb-sun16
    crashkernel=auto
    rd_LVM_LV=VolGroup/lv_root
    KEYBOARDTYPE=pc KEYTABLE=us rd_NO_DM
    rhgb quiet
  module /initramfs-2.6.32-431.5.1.el6.x86_64.img
  # module /list.data
```

4. Reboot using the new grub entry to gain access to the TPM.

5. Once the system has rebooted, verify that the **/dev/tpm0** character special device exists.

```
$ ls -l /dev/tpm0
```

6. Set the password on the TPM.

NOTE: You MUST choose a password that is exactly 20 characters long.

NOTE: Once the password is set, it can only be reset by clearing it in the BIOS. DO NOT FORGET THIS PASSWORD—it will be used in following steps!

NOTE: The '-z' option is important!

Execute the following command:

```
$ tpm_takeownership -z
```

7. Create the LCP and write the MLE hash to the TPM using the automated script:

```
$ create-lcp-tboot-policy.sh <20_character_
passwrd>
```

8. Edit **grub.conf** and uncomment the following line:

```
module /list.data
```

9. Reboot again using the new grub entry and verify that Intel TXT is now enabled on the system:

```
$ txt-stat | grep ‘measured\|secrets’
             secrets: TRUE
         TXT measured launch: TRUE
         secrets flag set: TRUE
TBOOT: measured launch succeeded
```

4.2 Changes to the MLE: Kernel, BIOS, Module Upgrades, Grub Boot Options

Maintenance of the Intel TXT environment is required as a part of regular system maintenance, such as upgrades of kernels and modules, addition of new hardware, and updates to BIOS. The following script must be executed when the BIOS, kernel, modules, or grub command line are changed:

```
$ update-tboot-policy.sh <20_character_passwrd>
```

5 OpenAttestation

OpenAttestation is an open-source project that was initiated by Intel. It provides a service to retrieve data provided by Intel TXT from remote systems, so that trusted compute pools can be defined based on trusted status of execution platforms.

5.1 OpenAttestation Server Installation

5.1.1 Enable epel/epel-oat/rhn base/rhn Optional Repositories

1. Add the EPEL repo config file into **/etc/yum.repos.d**:

```
$ rpm -Uvh http://download.fedoraproject.org/
pub/epel/6/i386/epel-release-6-8.noarch.rpm
```

2. Add the **epel-oat** repo config file:

```
$ wget http://repos.fedorapeople.org/repos/
gwei3/oat/epel-oat.repo && cp epel-oat.repo /
etc/yum.repos.d/
```

3. Add **rhn base/optional**:

```
$ rhn_register --nox --proxy=https://
proxy.<xxx>.com:<ppp>
```

NOTE: If not within an intranet environment, just “rhn_register --nox ”

```
Username: <rhn-username> Passwd: <rhn-password>
$ rhn-channel -a --channel='rhel-x86_64-
server-6' -u <rhn-username> -p <rhn-password>

$ rhn-channel -a --channel='rhel-x86_64-
server-optional-6' -u <rhn-username> -p
<rhn-password>
```

5.1.2 Installation

```
$ yum makecache
```

1. Configure iptables to accept the attestation service port (8443 is the default) and add the following line into **/etc/sysconfig/iptables**:

```
-A INPUT -p tcp -m state --state NEW -m tcp
--dport 8443 -j ACCEPT
```

Note: Should also be mirrored in ip6tables

2. Set SELinux to permissive mode: config selinux in **/etc/selinux/config**. For example:

```
SELINUX=permissive
Will update in future
```

3. On the server, install **oat-appraiser:**

```
$ yum install oat-appraiser
$ cd /usr/share/oat-appraiser/ && bash OAT_
configure.sh
```

4. On hosts, install oat-client (it can be installed on the same machine as **oat-appraiser**):

```
$ yum install oat-client
```

NOTE: Reserve 8443 as the default service port for attestation. If this port has already been occupied, redefine the port number on the server and client sides. The following steps are an example of what should be performed before executing **provisioner.sh**:

Server side:

$ sed -i “s/8443/8442/g” $TOMCAT_HOME/conf/server.xml

If there is multiple configuration for “Connector”, keep and modify the last one.

Client side:

$ sed -i “s/8443/8442/g” /usr/share/oat-client/script/OAT_client.sh

NOTE: If this is not the first time OpenAttestation has been deployed, remove the following leftover directories before installation:

/etc/oat-appraiser/
/etc/oat-client/
/var/lib/oat-appraiser/
/var/lib/oat-client/
/usr/share/oat-client/
/usr/share/oat-appraiser/

5.2 OpenAttestation Client Installation

1. Install oat-commandtool:

```
# yum install oat-commandtool
```

2. Copy **PrivacyCA.cer** and **TrustStore.jks** from appraiser to client:

a. Copy <**oat-appraiser-server>:/var/lib/oat-appraiser/ClientFiles/PrivacyCA.cer** to **<oat-client-host>:/usr/share/oat-client/**

b. Copy **<oat-appraiser-server>:/var/lib/oat-appraiser/ClientFiles/TrustStore.jks** to **<oat-client-host>:/usr/share/oat-client/**

NOTE: Repeat the above steps if you have redeployed your OpenAttestation appraiser.

3. **Run the provisioner script. Run provisioner.sh**:

Make sure you enter the hostname correctly the first time when prompted. If you make a mistake in the hostname, you must completely uninstall all OpenAttestation services and delete all left-over files and directories before you can reinstall correctly.

```
$ echo -n “<20-char tpm owner password>” |
xxd -p
<40-digit hex tpm owner password>
$ cd /usr/share/oat-client/script
$ sed -i  “s/111111111111111111111111111111
11111111/<40-digit hex tpm owner password>/g”
provisioner.sh
$ sed -i  “s/TpmOwnerAuth = 111111111111
1111111111111111111111111/TpmOwnerAuth =
<40-digit hex tpm owner password>/g” /usr/
share/oat-client/script/OAT_client.sh
$ bash provisioner.sh (make sure tcsd
service is running)
$ /etc/init.d/OATclient start
```

5.3 Node Whitelisting

The scripts referenced in this section can be found in the oat-commandtool RPM package.

5.2.1 Initial Installation

Register the node with the OAT appraiser:

```
# oat-whitelist-node.sh <oat appraiser fqdn>
<my ip>
```

5.2.2 System Maintenance and Upgrades

After upgrading the kernel, modules, bios, or grub command line options:

```
# oat-update-node.sh <oat appraiser fqdn>
<my ip>
```

6 OpenStack Configuration

The OpenStack controller nova-scheduler must be installed on bare metal in order to access the TPM, which is required to communicate via the OpenAttestation client with the OpenAttestation service to determine which compute node(s) are in the trusted pool. The controller system must be provisioned as a system in the trusted pool, but it must be registered with the OpenAttestation server to determine which OpenStack compute nodes have been provisioned as trusted pool nodes.

Before following this set of steps, prepare the environment as follows:

- **Have the OpenStack environment ready**, with at least two compute nodes.
- **Have the OpenAttestation appraiser service ready on a server**, and add one compute node as a trusted host.

NOTE: The following steps assume the default 8443 port is used for the attestation service. If the port is changed in the sections above, change it accordingly below.

1. Get **certfile.cer** using the following command:

```
openssl s_client -connect <OAT_APPRAISER_
HOSTNAME>:8443 | tee /etc/nova/certfile.cer
```

2. Verify that the node was added as trusted successfully using the following command:

```
curl --noproxy <OAT_APPRAISER_HOSTNAME> -v
--cacert ./certfile.cer -H “Content-Type:
application/json” -X POST -d ‘{“hosts”:[“<OAT_
CLIENT_HOSTNAME>”]}’ https:// <OAT_APPRAISER_
HOSTNAME>:8443/AttestationService/resources/
PollHosts
```

3. Modify **/etc/nova/nova.conf** for the nova-scheduler host by adding following items:

```
compute_scheduler_driver=nova.scheduler.
filter_scheduler.FilterScheduler
scheduler_available_filters=nova.scheduler.
filters.standard_filters
scheduler_default_filters=AvailabilityZone
Filter,RamFilter,ComputeFilter,TrustedFilter
[trusted_computing]
# attestation server name (string value)
server=<OAT_APPRAISER_HOSTNAME>
# attestation server port (string value)
port=8443
# attestation web API URL (string value)
api_url=/AttestationService/resources
# attestation server Cert file for Identity
verification
server_ca_file=/etc/nova/certfile.cer
# attestation authorization blob - must
change (string value)
attestation_auth_blob=oatoat
# Attestation status cache valid period
length (integer value)
auth_timeout=60
```

4. Add a new flavor for the trusted instance (the flavor for the image defines resources to be dedicated, such as the number of CPUs and the amount of system memory):

```
nova-manage flavor create m1.trusted 256 2
10 0 6 0 0
nova-manage instance_type set_key
m1.trusted trust:trusted_host trusted
```

5. Restart nova-scheduler and start a new instance with the new flavor:

```
nova --no-cache boot --flavor <id_of_
newflavor> --image <image_id> --key_name
<keypair> myinstance
```

7 Creating Trusted Instances with the Horizon Dashboard

Perform the following steps on the Horizon dashboard (for nova scheduler):

1. Go to **Project | Images and Snapshots**, choose the image to launch, and click launch.
2. On the next screen, choose **m1.trusted** as the flavor for the image, which will only launch new VMs on a host that has been verified as a trusted platform by OpenAttestation.
3. On the Horizon dashboard, navigate to the **Admin** panel and click **Instances** to show the running instances.
4. Verify that the **[named instance]** is running and that it is on the trusted server.

8 Conclusion

Red Hat Enterprise Linux OpenStack Platform provides an enterprise-ready option for IT organizations and cloud service providers to take advantage of Trusted Compute Pools based on Intel TXT and OpenAttestation. This approach combines the advantages of open source in terms of cost, flexibility, and innovation with the confidence of having Red Hat's industry leadership backing every aspect of the implementation.

The OpenAttestation package is planned for inclusion in future versions of Extra Packages for Enterprise Linux (EPEL), which will streamline installation for Red Hat Enterprise Linux, removing the need to install from source. (Including the package in Fedora is also planned).

Looking ahead, the long tradition of collaboration between Intel, Red Hat, and the open-source community portend ongoing advances throughout the solution stack, making Trusted Compute Pools on Red Hat Enterprise Linux OpenStack Platform an even more attractive option for securing the cloud.

Resources

- **Intel TXT white paper**:
  www.intel.com/content/dam/www/public/us/en/documents/white-papers/trusted-execution-technology-security-paper.pdf
- **Wikipedia entry on Intel TXT**: http://en.wikipedia.org/wiki/Trusted_Execution_Technology
- **Intel TXT Development Guide**:
  www.intel.com/content/dam/www/public/us/en/documents/guides/intel-txt-software-development-guide.pdf
- **Fedora* wiki entry on tboot**: https://fedoraproject.org/wiki/Features/Trusted_Boot
- **Fedora wiki entry on setting up OpenStack on a system with Intel TXT secure boot**:
  https://fedoraproject.org/wiki/OpenStackOnTXT
- **Scripts to ease Intel TXT/OpenAttestation deployment for OpenStack**: https://github.com/yocum137/txt-oat
- **Project page for tboot**: http://sourceforge.net/projects/tboot/
- **Project page for OpenAttestation**: https://01.org/openattestation
- **Intel TXT Enabling Guide**: http://software.intel.com/en-us/articles/intel-trusted-execution-technology-intel-txt-enabling-guide

[1] Press Release: Zenoss Reports On The State of Open Source Cloud Adoption.

[2] Gens, Frank, and John Gallant, Beyond the Hype: The Year in Cloud and Strategic Choices Ahead, Cloud Leadership Forum. https://www.eiseverywhere.com/file_uploads/d471b7932e4f64e622e9303eebd44848_CLF_2012_Opening_Remarks.pdf.

[3] No computer system can provide absolute security under all conditions. Intel® Trusted Execution Technology (Intel® TXT) requires a computer with Intel® Virtualization Technology, an Intel TXT-enabled processor, chipset, BIOS, Authenticated Code Modules, and an Intel TXT-compatible measured launched environment (MLE). Intel TXT also requires the system to contain a TPM v1.s. For more information, visit www.intel.com/content/www/us/en/data-security/security-overview-general-technology.html.

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT. UNLESS OTHERWISE AGREED IN WRITING BY INTEL, THE INTEL PRODUCTS ARE NOT DESIGNED NOR INTENDED FOR ANY APPLICATION IN WHICH THE FAILURE OF THE INTEL PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATH MAY OCCUR.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information. The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request. Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order. Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or by visiting Intel's Web Site www.intel.com.

Software and workloads used in performance tests may have been optimized for performance only on Intel microprocessors. Performance tests, such as SYSmark* and MobileMark*, are measured using specific computer systems, components, software, operations and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products. For more information go to www.intel.com/performance.

*Other names and brands may be claimed as the property of others.

0514/RJM/MESH/PDF 329201-001US