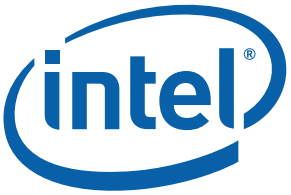

Scalable Trust Provisioning for Software Defined Architectures

Solution Architecture Document

March 2016

Revision 1.0
333992-001

Revision History

Revision	Date	Comments
1.0	March 1, 2016	Initial release (Intel Public).

Contents

NOTE: This page intentionally left blank.

1.0 Executive Summary

Enabling Trusted Compute Pool infrastructure usages, such as geographic fencing of workloads and infrastructure attestation, requires the setting of platform parameters close to the hardware. Specific BIOS settings such as the enablement of Intel® Virtualization Technology (Intel® VT-x and Intel® VT-d) and Intel® Trusted Execution Technology (Intel® TXT) need to be performed for every infrastructure host at least once during initial provisioning, and may require multiple boot cycles. This is a cumbersome process if done manually, often varying across server vendors. Therefore, this solution utilizes the Intel® Platform Trust Enabler (Intel® PTE) SDK integrated into an organization's IT infrastructure to automate this process, enabling bulk provisioning and unifying the process across multiple server vendors.

2.0 Business Requirements

Virtualization and cloud computing untie the close association of workloads and their underlying infrastructure. Workloads may, in general, be placed or relocated to any host in the infrastructure, thus relying on a split responsibility for the integrity of the software stack: the application owner is able to control the setup of the workload, while the infrastructure owner is responsible for any configuration in the lower layers. This distribution of security controls poses IT governance challenges when moving to the cloud, in particular in hybrid or public cloud scenarios. Addressing these governance challenges therefore becomes an important prerequisite for cloud service providers and IT departments looking to outsource workloads to cloud environments.

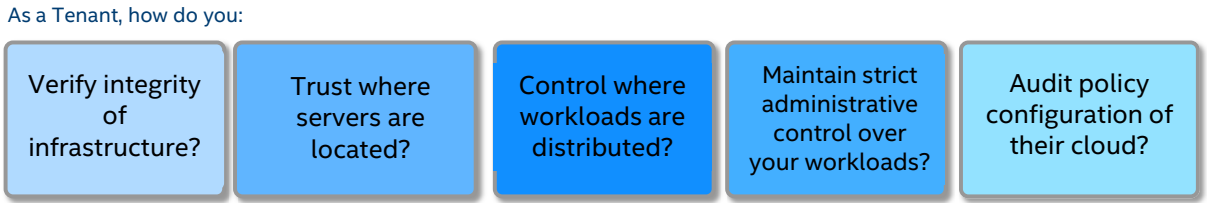

Figure 1. Questions to Consider

3.0 Trusted Computing as an Answer

This aforementioned loss of security control can be partially offset by automated boot time integrity checks, such as those offered by Intel® TXT which represents a hardware root-of-trust for measurement.

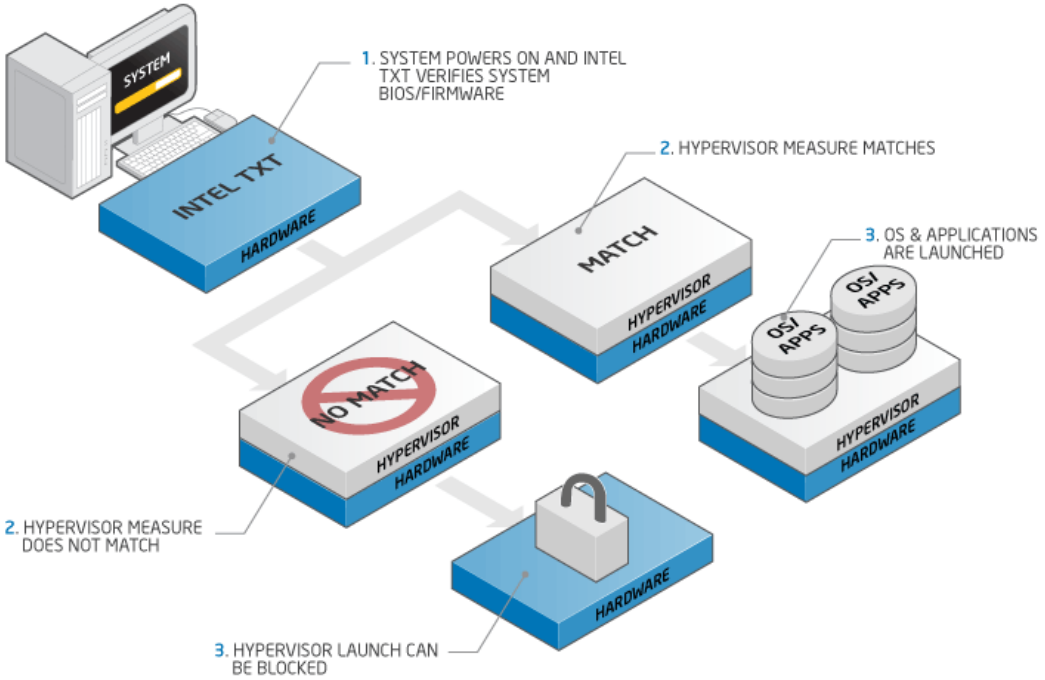

Figure 2. Intel® TXT Work Principle

After passing such checks during host boot time, a server is said to be trusted so that orchestration layers such as OpenStack* or vCenter*/vCloud* can utilize this attribute when automating workload scheduling.

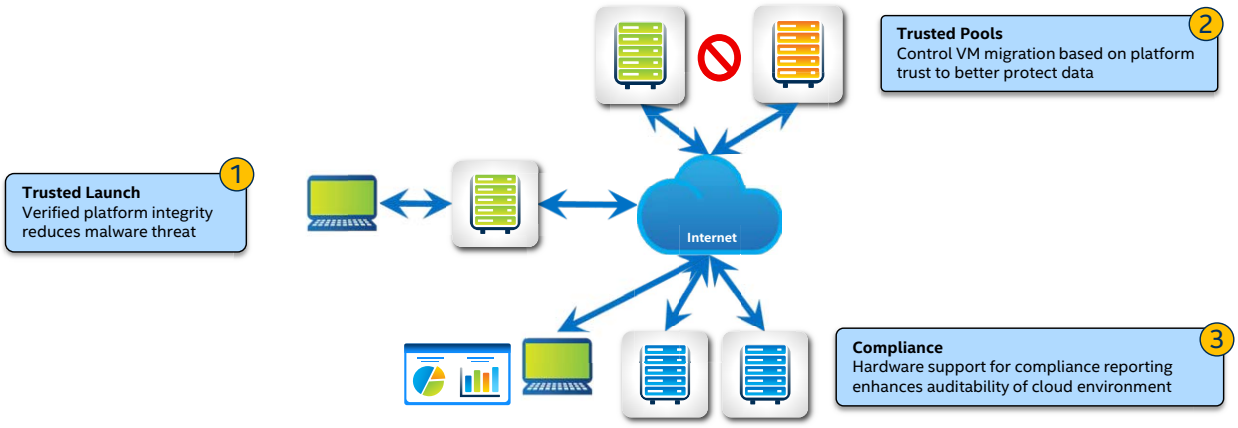

Figure 3. Usage Models Enabled by Intel® TXT

However, setting up a server system to be launched in this trusted manner requires the fulfillment of the following prerequisites:

1. A Trusted Platform Module (TPM) must be installed on the host's main board.
2. The correct firmware version must be installed.

3. The TPM must be activated in the BIOS.
4. Intel® Virtualization Technology and Intel® Trusted Execution Technology need to be switched on in the BIOS.

While item 1 must be performed when a server system is physically configured (for example, during assembly on the factory floor), items 2 through 4 are typically done via software.

Unfortunately, for these tasks to occur, most server system types must go through a number of reboot cycles (see Table 1), making this process slow and error prone if done manually.

Table 1. Reboots for Asset Tag Provisioning

OEM	Number of Reboots for Asset Tag PROVISION		Number of Reboots for Asset Tag RE-PROVISION	
	ESX	TA (Xen/KVM)	ESX	Xen/KVM
Cisco	5	2	5	2
Dell	5	2	5	2
Hitachi				
HP Blade	5	2	5	2
IBM	5	2	5	2
Intel	5	2	5	2
Quanta				
Supermicro	7	2	7	2
VCE				

4.0 Provisioning Solution Overview

In the following chapters we describe a solution to this setup and configuration challenge by a limited addition to data center and server landscape that uses industry standard best practices to automate items 2 through 4 across a range of machines and vendor types. This Intel® Platform Trust Enabler (Intel® PTE) is provided as a *Software Development Kit* (SDK) for customization to every data center customer's environment.

It is based on utilizing the PXE boot framework that exists in many IT infrastructures, and is aimed at automating the TPM provisioning, the activation of the Intel® TXT technology, and the provisioning of the asset tag information.

Intel® PTE 2.0 is a free software framework that has the flexibility to support multiple OEM's server types. It does so by relying on the vendor-provided host-based provisioning tools that will get called from a PXE-booted provisioning OS that is part of the Intel® PTE solution. This provisioning OS also coordinates provisioning steps with a centralized provisioning server and orchestrates the steps relevant for the local to-be-configured machine.

For this to work, Intel® PTE must rely on the following prerequisites:

- A trusted platform module must be installed and working. That is, its hardware provisioning must be done in advance.
- The machines that support Intel® TXT must be known in advance. Intel® PTE does not have the general capacity of detecting these capabilities.

In addition, Intel® PTE only takes care of the necessary firmware settings, but stops short of configuring the use of Intel® TXT in bare-metal installed OSs and hypervisors.

4.1 Functional Architecture

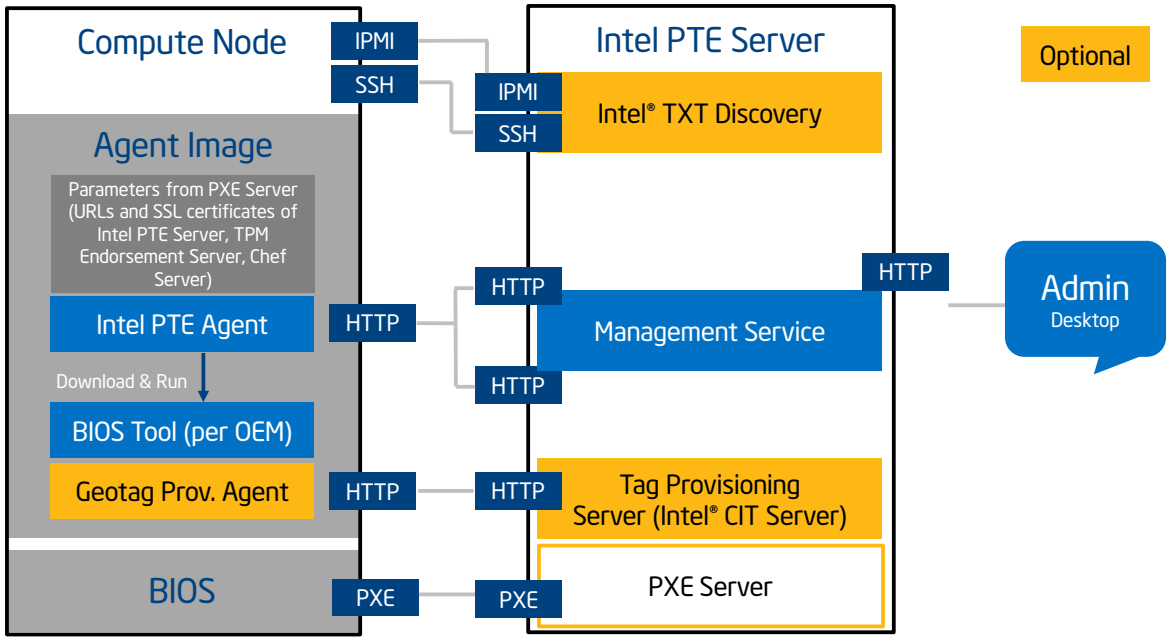

Figure 4. High-Level Functional Architecture

Servers in an infrastructure that are either re-imaged or re-purposed multiple times usually make use of a so-called PXE boot infrastructure. PXE is a standardized combination of DHCP and BOOTP/TFTP protocols. Central to this is a PXE server machine that acts as a DHCP server, issuing IP network addresses to servers requesting these during their network boot. In addition, it also hands out the pathnames to bootable image files to each individual host requesting this. When using this mechanism, an IT organization can ensure that individual boot images are delivered to machines based on their individual MAC Addresses, independent of the setup and configuration status of these machines.

The solution at hand utilizes boot images that are set up such that they take the server vendor's proprietary system configuration tool and orchestrate the different steps of the trust setup and configuration process. The image does so by connecting back to a new element in the network infrastructure, the Intel® Platform Trust Enabler server. This customizable virtual machine delivers bootable images that make use of each server vendor's proprietary system configuration tool, staging TPM enablement, and Intel® TXT as well as VT settings on each individual host. Coordination with the central Intel® PTE server occurs through a dedicated orchestration framework, using a client application in the target server's image and a central server application in the Intel® PTE machine. Hereby, a consistent state of provisioning is centrally maintained, even across the limited number of reboots that this configuration process as a whole requires.

During the course of this process, Intel® PTE additionally relies on well-known techniques such as IPMI and SSH to exercise tasks in power management and remote control.

In addition to the aforementioned settings, Intel® PTE can also automate the setting of a geographic tag within the TPM, which in turn can serve as an additional attribute in the trusted workload scheduling stage of cloud environments.

The activation flow that Intel® PTE executes for every hosts is shown in Figure 5.

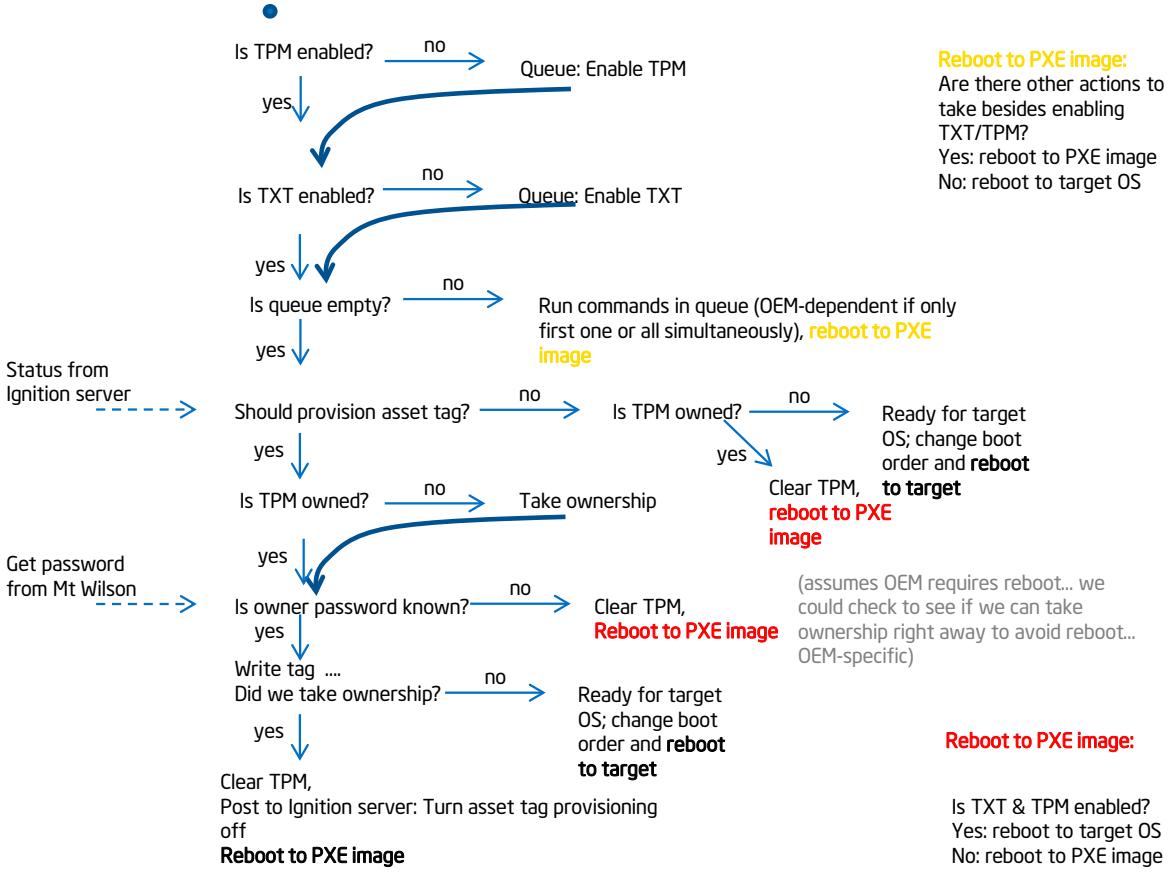

Figure 5. Intel® PTE Activation Flow

Intel® PTE currently offers to automate the provisioning of single hosts as well as a list of hosts. Required data can be put in interactively via browser-based masks from an administrative station, or can be uploaded in bulk via a spreadsheet into its main portal, again from an administrative workplace or from an API.

4.2 Technical Requirements

Since Intel® PTE 2.0 can be downloaded as a single-file installer binary, the following prerequisites must be met to set up this functionality for a given server vendor's machines:

- Ubuntu 12.04 VM to install PTE2.0 binary file.
- Appropriate OEM system configuration tool(s).
- An existing corporate PXE Server Environment.
- To be configured Intel® TXT-capable machines that can be connected to via a baseboard management controller (BMC) and that should be in a powered-off state before beginning this process.

5.0 Deploying the Intel® Platform Trust Enabler SDK

Intel® PTE 2.0 comes as a 190 MB binary file that must be executed on the Ubuntu virtual machine. During the installation of the Intel® PTE server, the administrative user must choose one of the following two deployment models:

- Most commonly, in a "Separate Services" model, the Intel® PTE server is the only application installed on a particular VM and handles Node Management only (that is, it orchestrates the various steps to be performed). For that it utilizes the corporate PXE server to provide the appropriate image, and utilizes the corporate attestation services (for example, Intel® Cloud Integrity Technology) to execute TPM Endorsement and the provisioning of the Asset Tag. The installation of either of these two (PXE server and Attestation Service) are not in the scope this document.
- In smaller environments, the "All-in-one" model can be used, and the Intel® PTE server is installed on the same OS instance alongside the corporate PXE server and an attestation service. All functions of the provisioning process are combined on a single machine:

An example implementation of the "Separate Services" deployment architecture for hosts of three different vendors is shown in Figure 6:

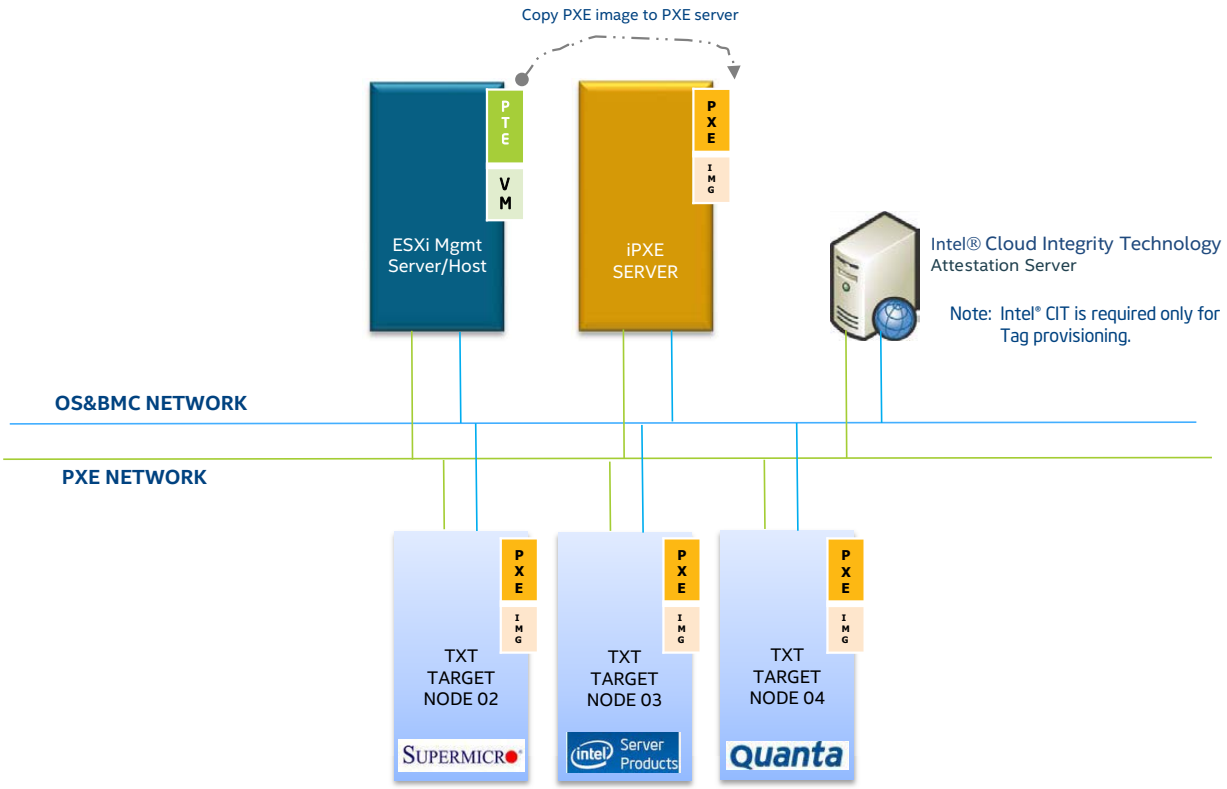

Figure 6. Separate Services Deployment Architecture

6.0 Configuring and Executing Intel® PTE

To prepare the provisioning infrastructure for each type of to-be-activated host, the following steps must be taken:

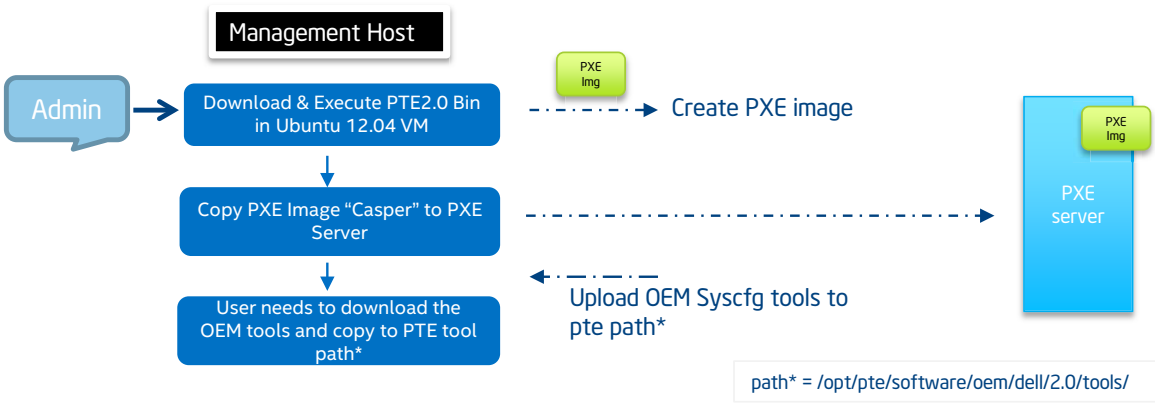

Figure 7. Intel® PTE Preparation

Once the corresponding PXE boot image for that particular server type has been prepared and uploaded to the PXE server, the process of provisioning Intel® TXT on one or more of these types of hosts can be triggered:

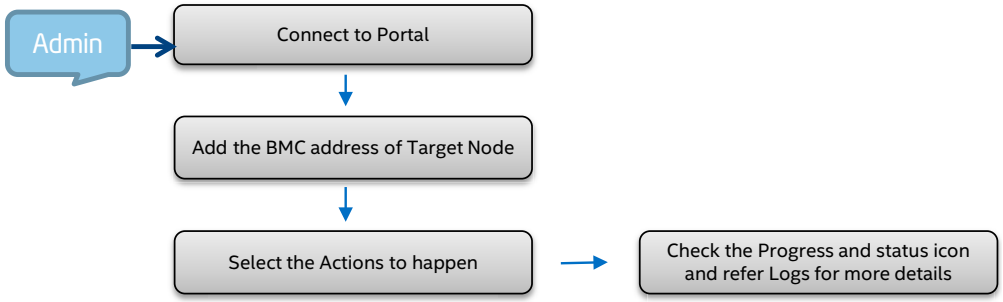

Figure 8. Intel® TXT Provisioning

7.0 System Support

Currently, Intel® PTE can be used with server platforms of the following vendors:

Table 2. Vendor Support

OEM	TXT/TPM Activation	ATAG Provisioning	Tools Required	Licenses	Comments
Dell	Yes	Yes	DTK [Dell Deployment Tool Kit]	Free	Validated on Romley Platform
HP	Yes	Yes	CONREP	Free	Validated on Romley Platform
Intel PCSD	Yes	Yes	SYSCFG [sysconfig]	Free	Validated on Romley Platform
Quanta	Yes	Yes	AFULNX	Free	Validated on Romley Platform
Supermicro	Yes	Yes	SUM [Supermicro update Manager]	Paid license per node for SUM	Validated on Romley Platform

NOTE: This page intentionally left blank.

LEGAL