Integrated OpenStack™ Cloud Solution with Service Assurance

Executive Summary

- Enterprise IT needs an integrated certified hardware/software solution for faster deployment of private cloud applications.
- Customers want to avoid vendor lock-in. OpenStack™ provides a path where multiple vendor solutions can be deployed to get the best value for IT dollars. Redapt and Intel have created an optimized reference solution by combining their expertise enabling faster deployment, maintenance, and operation of a cloud solution based on OpenStack on Intel® Xeon™ based servers for your corporate environment.
- The private cloud must also be able to run all workloads. This includes elastic cloud native applications, as well as enterprise workloads that require higher levels of trust and predictability of performance.

Solution Overview

- **Certified Hardware**: Optimized for customer cloud needs
- **OpenStack**: No vendor lock-in; enhanced for service assurance administration
- **Stable Roadmap**: Establish path to tap Intel innovation in future platform technologies

**Audience**

This white paper is targeted to enterprise IT architects, cloud services providers, and decision makers who are exploring deploying cloud-based solutions in their enterprise to meet increasingly elastic compute resource demands from customers that must support enterprise workloads.

**Challenges and Pain Points**

- **Running both new applications and enterprise workloads** on private cloud, while adding service assurance administration for trust and performance

---

“Multitenant environments bring workload challenges and Intel® Service Assurance Administrator helps address the main concerns of security and performance.”

— Jeff Dickey, Senior Vice President of Cloud Solutions, Redapt
Why Cloud Computing for the Enterprise?

Enterprises are pushed to spend less money at the same time technology and operations become more extensive. Traditional roles are shifting, with IT professionals becoming “generalists” with less time to be fully trained on the vast number of new and evolving technologies. Despite the marketing, cloud is extremely complex and takes many vendors all working together to create a successful production cloud. IT managers are looking to deploy Openstack for a number of reasons, including:

- Enables deployment of extensible, flexible, and resilient cloud infrastructure
- Provides the most impact for the cost
- Maximizes business agility
- Leverages an open architecture that promotes flexibility and investment protection
- Avoids proprietary vendor lock-in

OpenStack Shift

The open-source program Openstack is picking up momentum from large Industry companies. Equipped with versatile use cases and lower cost of entry, it is emerging as a large player in the cloud computing space. With Openstack, legacy infrastructure limitations are removed via next-gen architecture. Openstack provides the building blocks for distributed applications. Enterprises are rapidly moving from client server infrastructure to distributed cloud applications. This shift is due to the complexity behind distributed cloud applications: many companies do not have the production cloud to develop these applications.

Why Move Applications?

There are many reasons to move your applications to a cloud platform. The most common is to increase agility and scalability. The cloud minimizes downtime because applications are resilient. This also allows management to make faster business and technology decisions, pivoting products and scaling out to insure reliable performance for application users.
Why Move to Openstack?

With technology changing rapidly, business units are moving at an exponential rate. Management is leaning away from traditional vendors for their business and technology needs. This is enabling greater buyer flexibility and business agility. Openstack innovation is outpacing the speed of adoption. The key is to incorporate Openstack with Intel SAA to meet the demands of mixed workload enterprise environments. Intel SAA fills a critical gap for IT when implementing Openstack at the enterprise level. Intel SAA enables workloads to run securely, with consistent performance, and enables SLA monitoring and cloud capacity provisioning and monitoring. Redapt provides operations training for your Openstack and Intel SAA cloud environment.

Public clouds have been widely discussed and have distinct benefits. However, performance reliability can be spotty at best. Public clouds do not enable building scale-out cloud applications without an enterprise-class development platform. Openstack is built for next-generation applications (Intel SAA helps to allocate and manage VMs that are supporting legacy apps). Redapt and Intel are working with customers to ensure maximum control of their infrastructures. Redapt and Intel can work with your team in capacity management and application SLAs. We can help eliminate vendor lock-in and vendor dependency. Redapt and Intel solutions enhance out-of-the-box OpenStack cloud distributions.

Redapt and Intel Openstack and Intel SAA Hardware Setup

- **Openstack Pod**: 21 servers total. Six management nodes, 10 compute nodes, and 5 storage nodes (2 Proxy, 3 storage nodes)
- **Spine Network**: Force10 S6000 switches connected to Force10 S4810 switches
- **Leaf Network**: Force10 S4810 switches connected to Intel® Ethernet Server Adapter X520-DA2 dual 10GbE NIC on every node
- Each server has an internal private Intel® dual 1GbE NIC connected to a top-of-rack switch that is used for management tasks
- Each compute node is populated with 6 10K, 600GB hard disk drives for a total of 3.6TBs of raw storage per server
- Each compute node is also populated with 2 Intel® 320GB SSD drives
- Two Intel® Xeon® E5-2660 v2 2.20GHz, 25M cache, 8.0GT/s QPI, Turbo, HT, 10C, 95W, maximum memory
- 128GB of 1600MHz DDR3 memory
Intel® Service Assurance Administrator (Intel® SAA) Fully Integrates with OpenStack

Intel SAA software consists of three components: Controller, Agents, and an OpenStack scheduler Plug-In. The Controller periodically collects deep platform telemetry data from compute node Agents to enhance virtual resource scheduling decisions. The Plug-in for the OpenStack resource scheduler connects to a Controller virtual appliance that routes machine instance provisioning requests for “machine flavors” with service level enhancements to compute nodes that match the required trust and performance objectives. The RealTimeAnalysisEngine (RTAE) in Intel SAA also monitors the state of the system, detects violations of SLAs within seconds, and alerts the administrator. Finally, SLA compliance reports can be generated to provide a record of compliance. The result is an assurance engine that provides a level of confidence that the cloud machine instances continue to run and meet their service level objectives.

Intel SAA integrates seamlessly into OpenStack. The user can switch from the Intel SAA UI to the OpenStack Horizon UI right from the dashboard. Once in the Horizon UI, the user can launch virtual machines (VMs), access the flavors available in OpenStack and define additional flavors in Intel SAA. (A flavor is the OpenStack name for a virtual hardware template). Switching back to the Intel SAA UI allows the user to monitor the nodes and VMs launched on them.
Enhance Cloud Services Catalog with Enterprise-Grade SLA Machine Flavor Creator

For applications to perform as expected, they often establish an SLA with the infrastructure. The SLA specifies required compute performance, I/O throughput and latency, amount of memory, security objectives, and other requirements.

For the service provider or IT group, implementing this SLA can be challenging. For example, the resources that an application uses locally on a bare-metal server are not impacted by applications on other (bare-metal) servers. But in a virtualized, multitenant environment, applications are co-residing with other applications on shared infrastructure. Ensuring the performance of applications to meet the target SLA, while also ensuring that other applications do not interfere, is not a simple task.

When a virtual machine is presented to OpenStack for instantiation, a flavor is associated with the virtual machine (a normal function for OpenStack). Intel SAA enables the cloud administrator to attach a set of service level objectives (SLOs) to the flavor. When a virtual machine instance is created using that flavor, the Openstack scheduler passes the request on to the Intel SAA Scheduler Plug-in, which in turn:

- Determines the specified performance requirements, measured as Service Compute Units (SCU), based on the flavor and the required trust
- Determines the compute node best suited to host that application based on the compute node current loading, current levels of contention, and attested trust

Service Compute Unit (SCU) is a function of processor frequency, throughput, instruction set efficiency, and cache.

OpenStack installations with Intel SAA can enhance OpenStack flavors with additional service level objectives for trust and performance. Intel SAA software provides monitoring, remediation, and reporting capabilities to assure that applications continue to run and to meet their SLA. Flavors are created in the Intel SAA UI and are available as new flavor options in the OpenStack UI. This allows the user to launch VMs from the OpenStack UI and select these new flavors from the available options. In the figures on page 6, the flavors created in the Intel SAA UI are also displayed in the OpenStack UI.

“Customers are asking for another option—OpenStack with Intel® Service Assurance Administrator gives them open source with confidence.”

Jeff Dickey,
Senior Vice President
of Cloud Solutions, Redapt
Enhance Capacity Management and Planning

The introduction of the SCU and its use in Intel SAA provides greater clarity for cloud infrastructure capacity management and planning. The capacity and current utilization of a compute host based on the actual VMs running on the host are measured in SCUs.

In the Intel SAA UI, the cloud administrator can monitor the utilization of the compute hosts in the cloud and plan for adding capacity as well as migration of VMs, if necessary. The figure below is a section of the Nodes tab of the UI showing the utilization of the total capacity, as well as the cache contention on each node.

Openstack Dashboard
Enhance Monitoring and Remediation

From the Intel SAA UI one can monitor the health of the critical components that comprise the OpenStack infrastructure. The dashboard below gives a high-level view of the health of the various components. If needed, one can dive into specific components to determine the exact failure status and restart the component.

Aggressor-Victim Detection

A prevalent issue in public clouds is the inability to gain clarity on why a particular instance of a VM may not perform to the SLA expectations. Oftentimes, this may be the result of resource contention by other VMs running on the same host. This problem is defined as the noisy neighbor problem. An aggressor VM (or VMs) causes poor performance by the victim VM. In the Intel SAA UI, the cloud administrator can identify both aggressors and victims. Furthermore, it is possible to identify which aggressor(s) are responsible for the victim’s poor performance, enabling easier root causing and remediation.
Enhance Provisioning of Cloud machines (VMs) with Intel® Trusted Execution Technology (Intel® TXT)

Intel® Trusted Execution Technology (Intel® TXT) provides hardware-based security to help build a solid foundation for security. Built into Intel’s silicon, Intel TXT technologies address the increasing and evolving security threats across physical and virtual infrastructures by complementing runtime protections such as anti-virus software. Intel TXT can also play a role in meeting government and industry regulations and data protection standards by providing a hardware-based method of verification useful in compliance efforts.

Intel TXT is specifically designed to protect platforms from the emerging threats of hypervisor attacks, BIOS, or other firmware attacks, malicious root kit installations, or other software-based attacks. It increases protection by allowing greater control of the launch stack through a Measured Launch Environment (MLE) and enabling isolation in the boot process. More specifically, it extends the Virtual Machine Extensions (VMX) environment of Intel® Virtualization Technology (Intel® VT), permitting a verifiably secure installation, launch, and use of a hypervisor or operating system (OS). Intel TXT gives IT and security organizations important enhancements to help ensure more secure platforms; greater application, data, or virtual machine (VM) isolation; and improved security and compliance audit capabilities. Not only can it help reduce support and remediation costs, but it can also provide a foundation for more advanced solutions as security needs change to support increasingly virtualized or multitenant shared datacenter resources.

Intel SAA includes a built-in trust attestation engine that makes it easy to launch VMs on trusted nodes. When a server boots, the BIOS and VMM are checked against a known good configuration and a trust status is established. This trust signature is tamper-resistant and cryptographically secure. When the user selects an SLA which requires an enhanced machine flavor with trust, the scheduler selects a host from the collection of available machines which have been booted with Intel TXT enabled and the BIOS and VMM have been attested.

The figures above show that Node-15 is a trusted host and a VM (BV-10secure-gips) was placed on that node because the flavor selected for its SLA was secure-silver.
Integrated OpenStack™ Cloud Solution with Service Assurance

Redapt is a full service systems integrator that delivers innovative datacenter infrastructure and cloud solutions tailored to meet your business goals. We develop and integrate customized, best-of-breed, technology solutions that effectively address the business objectives of our clients, while lowering TCO and providing maximum investment protection. Learn more at: www.redapt.com.

Intel is a world leader in computing innovation. The company designs and builds the essential technologies that serve as the foundation for the world’s computing devices. As a leader in corporate responsibility and sustainability, Intel also manufactures the world’s first commercially available “conflict-free” microprocessors. Additional information about Intel is available at newsroom.intel.com and about Intel’s conflict-free efforts at conflictfree.intel.com.

Conclusion

Openstack is an exciting new technology inflection point for enterprise IT. To properly utilize it there has to be a smooth transition from existing ways of doing things to the cloud. Together, Redapt and Intel SAA offer a clear path to running enterprise applications with enterprise-level SLAs on an Openstack foundation with compute, trust assurance, and portability across heterogeneous infrastructure elements.

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.
Intel® Virtualization Technology (Intel® VT) requires a computer system with an enabled Intel® processor, BIOS, virtual machine monitor (VMM) and, for some uses, certain platform software enabled for it. Functionality, performance, or other benefits will vary depending on hardware and software configurations and may require a BIOS update. Software applications may not be compatible with all operating systems. Please check with your application vendor.
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.
A “Mission Critical Application” is any application in which failure of the Intel PUSE INTEL’S PRODUCTS FOR ANY SUCH MISSION CRITICAL APPLICATION, YOU SHALL INDEMNIFY AND HOLD INTEL AND ITS SUBSIDIARIES, SUBCONTRACTORS AND AFFILIATES, AND THE DIRECTORS, OFFICERS, AND EMPLOYEES OF EACH, HARMLESS AGAINST ALL CLAIMS, COSTS, DAMAGES, AND EXPENSES AND REASONABLE ATTORNEYS' FEES ARISING OUT OF, DIRECTLY OR INDIRECTLY, ANY CLAIM OF PRODUCT LIABILITY, PERSONAL INJURY, OR DEATH ARISING IN ANY WAY OUT OF SUCH MISSION CRITICAL APPLICATION, WHETHER OR NOT INTEL OR ITS SUBCONTRACTOR WAS NEGLIGENT IN THE DESIGN, MANUFACTURE, OR WARNING OF THE INTEL PRODUCT OR ANY OF ITS PARTS.
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.
© 2014, Intel Corporation. All rights reserved. Intel and the Intel logo 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.