Intel® Service Assurance Administrator

Product Overview

Running Enterprise Workloads in the Cloud

Enterprise IT wants to …

- Start a private cloud initiative to service internal enterprise customers
- Find an easy way to run enterprise workloads over a virtualized and cloud infrastructure while meeting service level objectives
- Explore open standards hardware and software cloud solutions to increase vendor choices, potentially reduce cost, and increase access to innovation

… but setting up and operating a cloud can be difficult

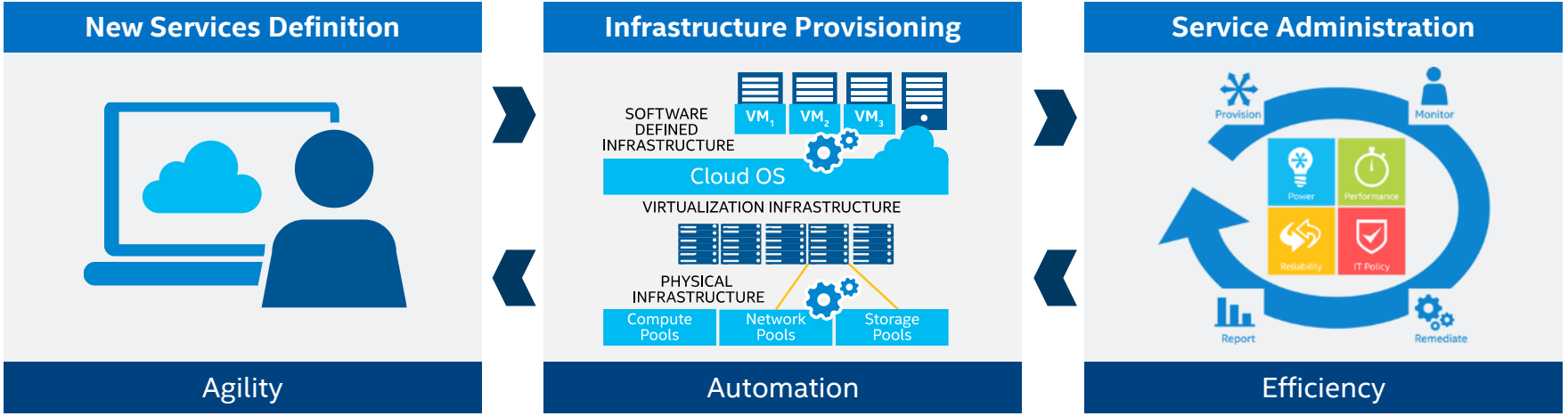
New cloud services and infrastructure monitoring tools and capabilities are required to meet enterprise service level objectives

Challenges Running Enterprise Workloads in the Cloud

Enterprise Workloads Require cloud services and a robust infrastructure.

- **Trust:** Is my workload running on trusted multitenant infrastructure? How do I know that BIOS and hypervisors are not compromised (trust attestation)?
- **Performance:** Will my workload get expected compute cycles? How do I avoid “noisy neighbors”?
- **Availability:** Is it possible to find and address root cause of issues in cloud infrastructure and services? Is the hardware and software open for innovation?

Software-Defined Infrastructure Needs Service Administration

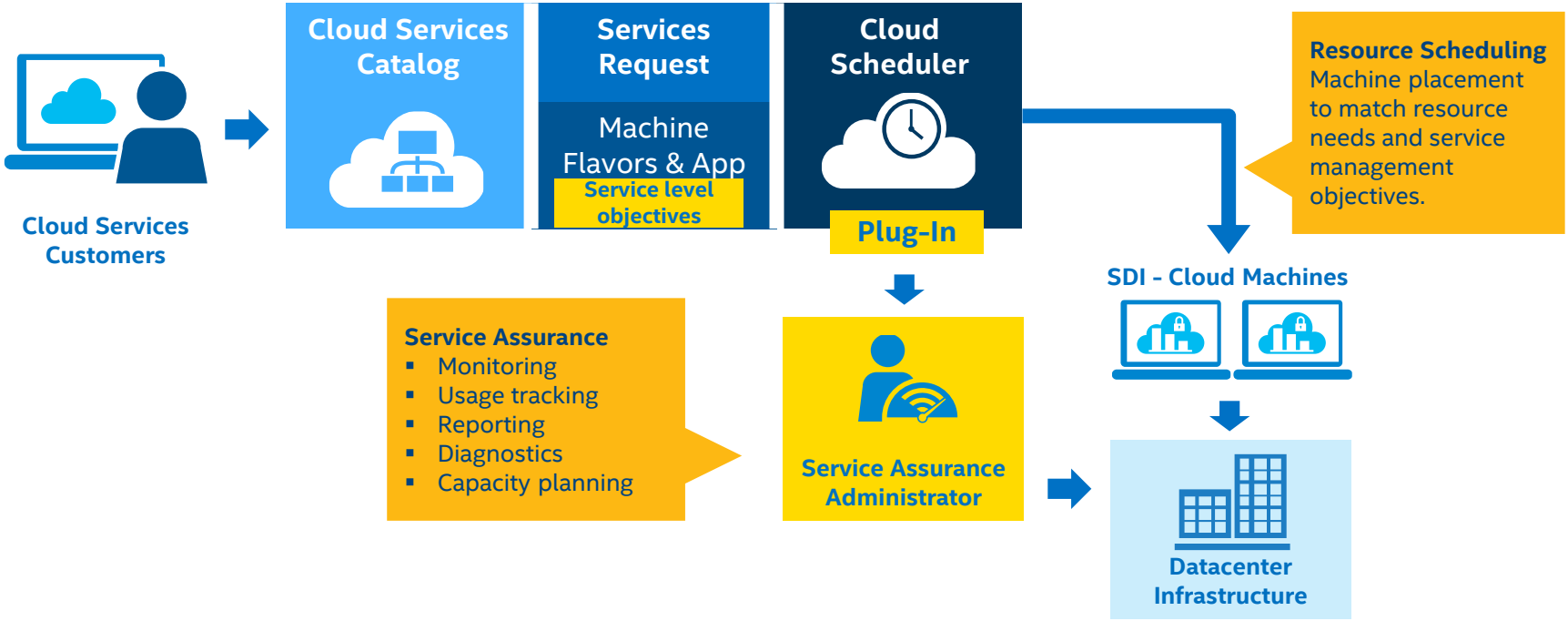


Enterprise workloads need service assurance for cloud services and infrastructure

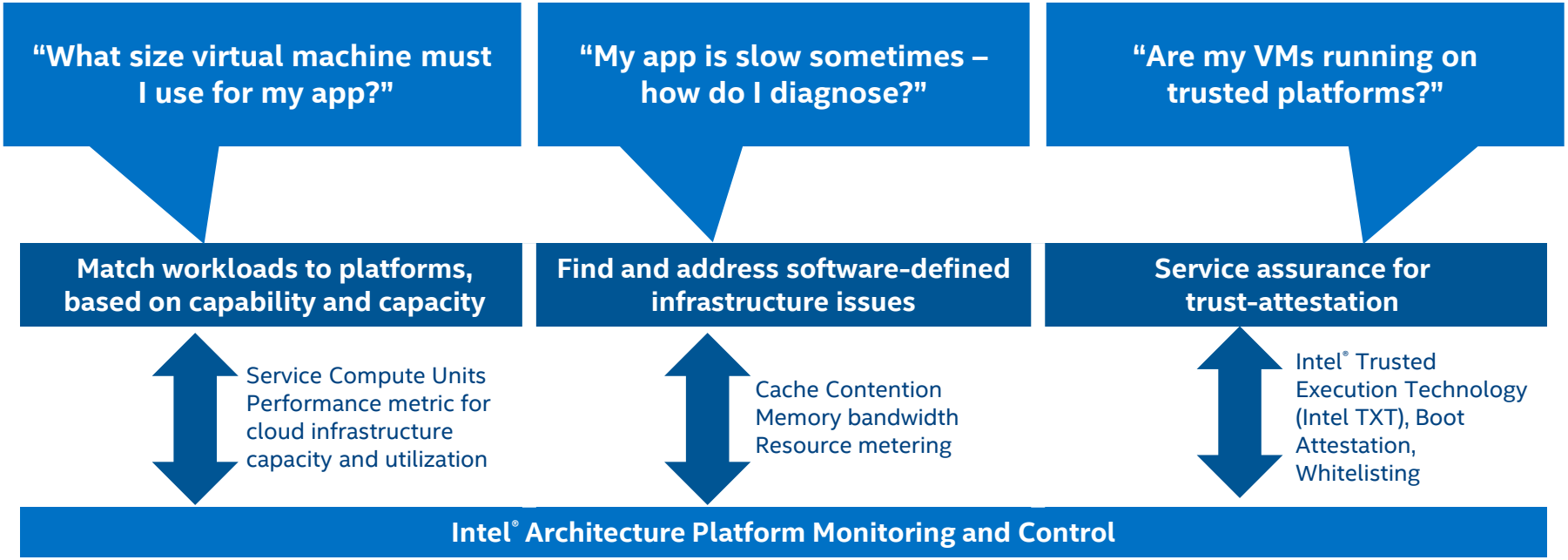
- Deploy workloads quickly using software-defined infrastructure
- Achieve target service level objectives
- Minimize "blamestorming" on cloud infrastructure issues

Cloud infrastructure can be enhanced with service assurance administration software tools to run enterprise workloads efficiently.

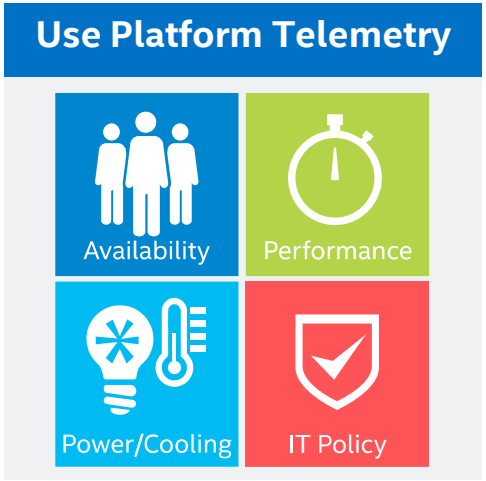
Cloud Service Assurance Overview

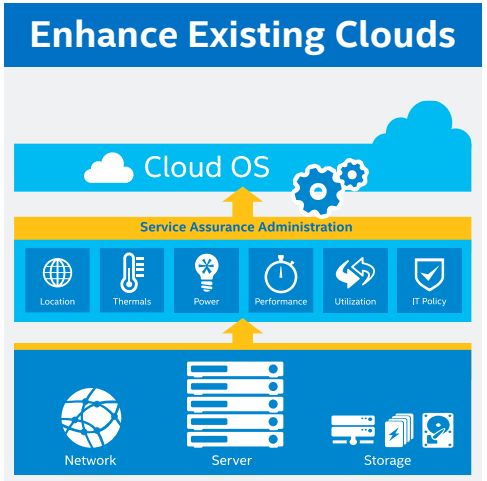


Why Intel® Service Assurance Administrator?

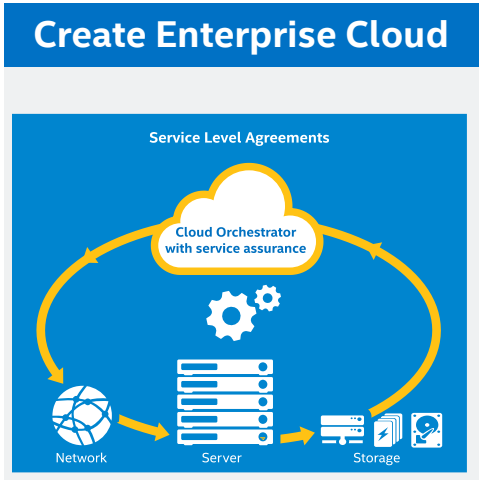


Cloud Infrastructure and Services Solution Options



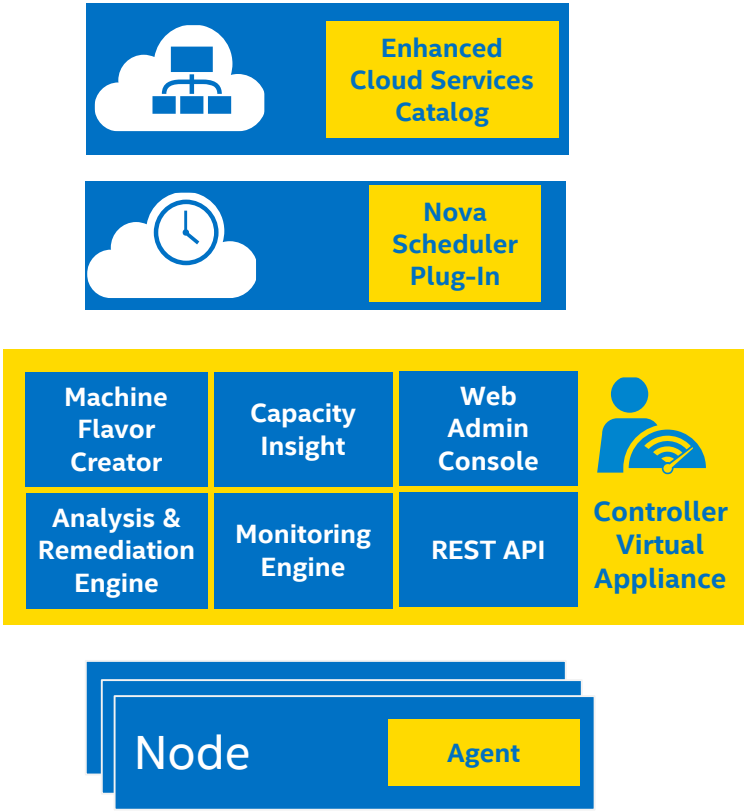


OR



- Have an OpenStack Cloud already? Enhance it with service assurance administration
- You need a turnkey cloud solutions? Make sure it integrates service assurance administration software tools

Intel® Service Assurance Administration Feature Highlights



- **Intelligent Machine Placement with Automated Provisioning**
  - Enhance Machine Flavors managing to service level objectives
  - Instances scheduled on trust-attested compute nodes
  - Instances scheduled to meet compute performance quotas
- **Probable Root Causing with Analysis & Remediation Engine**
  - Monitoring of critical OpenStack compute components
  - In-depth compute node monitoring to detect anomalies, set/execute IT policy, collect service level violation data
- **Insightful planning with Capacity and Usage Data Reporting**
  - Compute node capacity, capability and consumption
  - VM capacity, capability and consumption
  - Reporting for enhanced IT Policy compliance –Machine Instance provisioning instantiation, node trust-attestation status, performance metrics

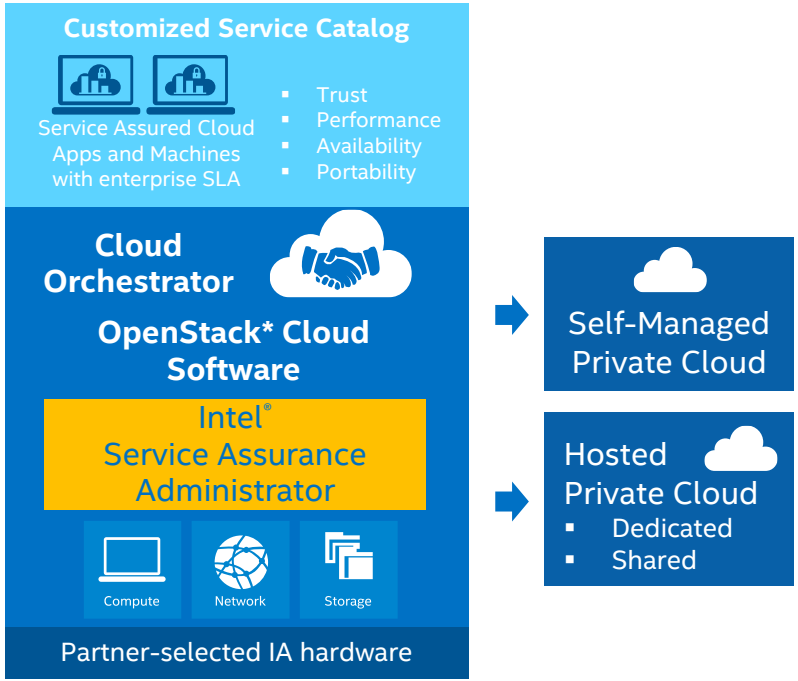
Intel® Service Assurance Administrator

Features	Benefits
Enhance Machine Flavors managing to service level objectives	▪ Target machine instances to run only on trust-attested compute nodes ▪ Specify performance quota with Service Compute Unit enabling higher density of VM per node
Automated provisioning with intelligent machine placement	▪ Automated placement of VMs on trust-attested nodes ▪ Automated placement of VMs to avoid performance issues
OpenStack* Health Monitoring: Efficient Administration	▪ Critical OpenStack component monitoring ▪ In-depth compute node monitoring
Analysis and Remediation Engine: Probable Root Cause Analysis	▪ Log file data collection ▪ Detect anomalies ▪ SLA violation detection
Capacity and usage for insightful planning	▪ Compute node resource capacity, capability, and consumption ▪ VM capacity, capability, and consumption ▪ Intelligent, automated machine instance provisioning

Intel® Service Assurance Administrator

Features	Benefits
Reporting Engine for IT policy compliance and auditing	▪ Machine instance provisioning: instantiation reports ▪ BIOS and Hypervisor Trust-attestation reports ▪ Performance metrics reporting
Service Assurance Engine – Easy OpenStack* Integration	▪ **Plug-in:** enhances nova-scheduler* to assure automated and efficient machine instance execution ▪ **Controller:** virtual appliance (KVM) that serves as a central monitoring and management engine for a cluster of cloud infrastructure ▪ **Agent:** platform telemetry for compute node running Linux* ▪ **Service assurance API:** REST* interface enables easy integration with existing IT operations tools ▪ **Administration console:** skin the Web UI, built using service assurance API

Creating an integrated cloud solution with Intel® SAA



- Steps to create a private cloud with Intel® SAA
  - Install OpenStack* on selected datacenter infrastructure
  - Provision bare-metal servers with Linux* and KVM*
  - Install object and block storage solutions
  - Install agents to monitor the solution components
  - Enable service assurance management
  - Support HA deployment
  - Monitor and manage solution including OpenStack components and service assurance administration software

Resulting solution enables a customizable cloud services catalog with enterprise-grade SLA for cloud machines and apps

Monitors, remediates, and reports on service-level objectives of physical and virtualized cloud infrastructure

Creates an integrated cloud solution where you can monitor and manage service level objectives.

Intel® Service Assurance Administrator Summary

Agility

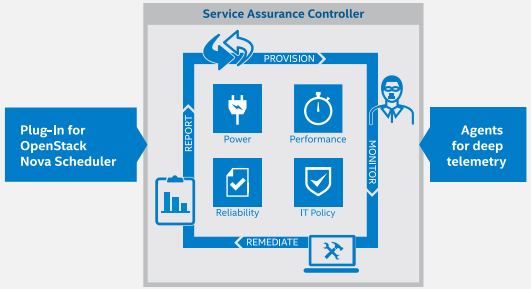
Run workloads with confidence on software-defined infrastructure

Enhanced Machine Flavors

Agile business service deployment

Automation

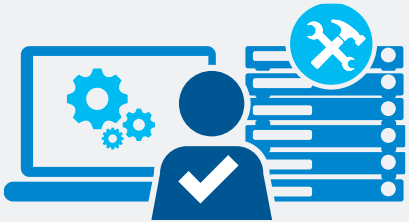
Enhance OpenStack* to provision and monitor machine flavors with specified service levels



Automated software-defined infrastructure

Efficiency

Integrate with IT operations tools to determine probable root cause, report, and help remediate issues



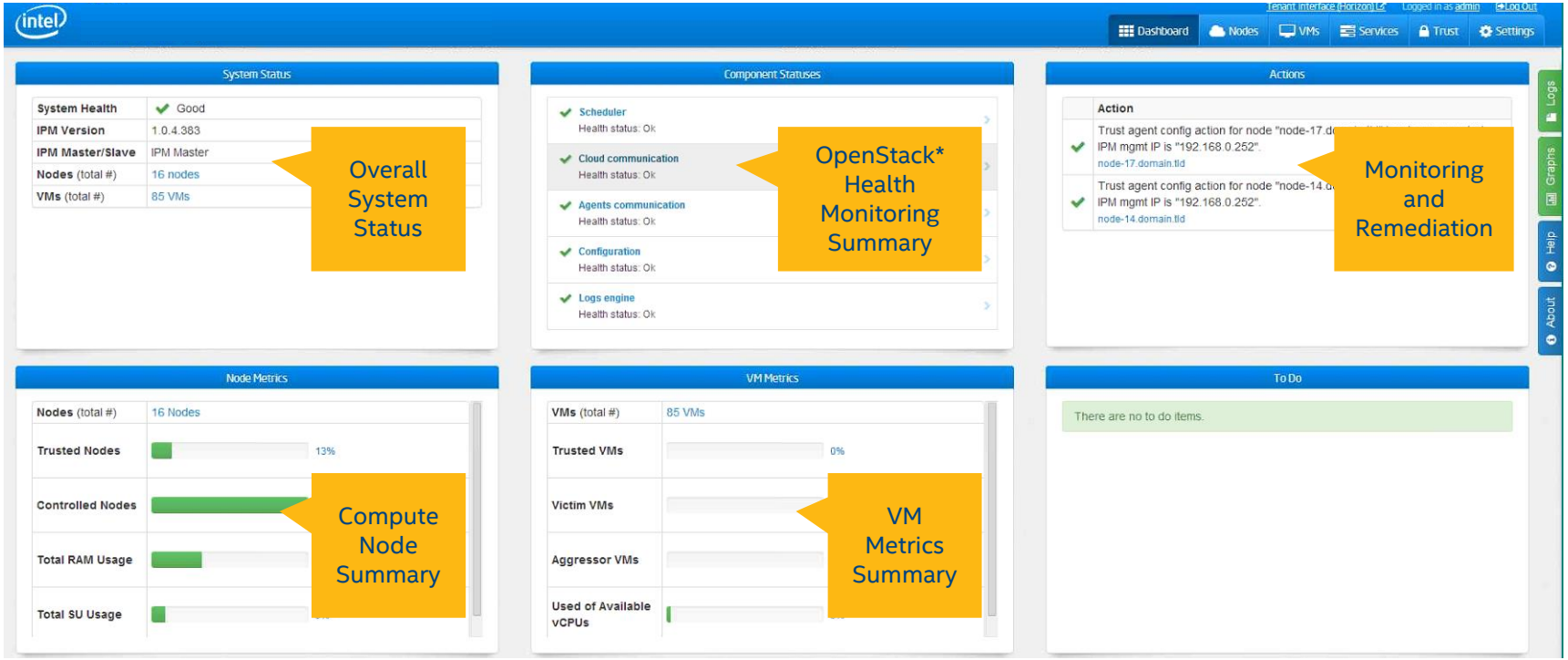
Efficient service assurance and administration

Intel®

Service Assurance Administrator Usages

Intel Confidential — Do Not Forward

Intel® Service Assurance Administrator Console Overview



Enhanced Machine Flavor Creator

Pain Points

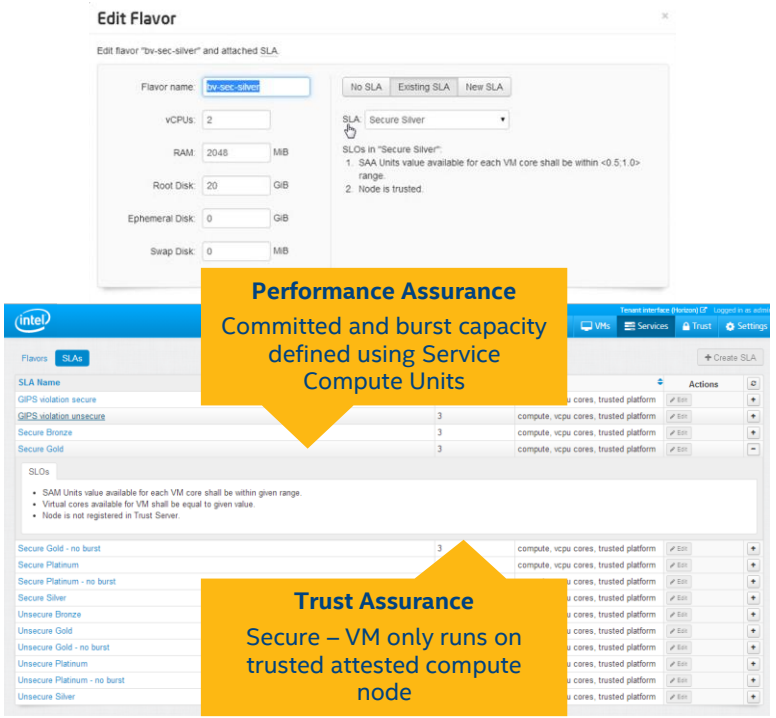
How can I assure my users that their cloud machine instances will run efficiently in a multitenant OpenStack* cloud environment?

Features

- Machine instances run on trust-attested nodes
- Performance assurance with target service level objectives using allocated/burst Service Compute Units (SCUs)^

Solution Steps

- Admin can define machine flavors using the machine flavor creator
- New machine flavors can be automatically published to OpenStack cloud services catalog
- Cloud customers select new flavors using OpenStack Horizon console or APIs
- An OpenStack Nova plug-in intercepts requests for new machine flavors and provisions machine instances using analytics
- Cloud administrator collects assurance reports for each machine instance
  - Review “provisioning instantiation” reports
  - Trust attested compute pools compliance reports
  - Performance metrics reports



^Service Compute Unit (SCU) provides a performance measure of capacity and consumption of IA compute across generations of IA processor

Efficient Administration with OpenStack* Health Monitoring

Pain Points

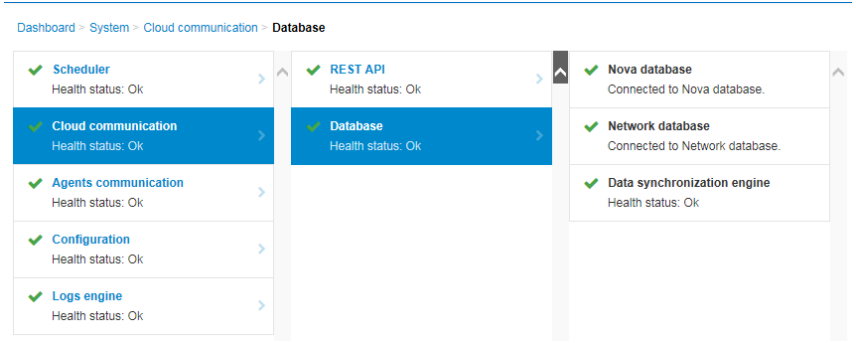
- How can I tell if OpenStack components are running?
- Which OpenStack component is the probable root cause of issues?

Features

- Monitors critical OpenStack components
- Simple-to-use visual display for OpenStack administrator

Solutions

- Administrator visits the console dashboard and visually inspects any alert notifications
  - ✓ Determination of probable root cause of issues by operator by identifying OpenStack component failures
  - ✓ Makes information readily available to administrator
- Alternatively, IT Operations Management software can connect to the controller using RESTful API and gather OpenStack issues data to execute automated/manual response procedures



Capacity and usage data for insightful planning

Pain Points

- Is the current compute capacity enough to meet workload needs?

Features

- Compute node capacity, capability, and consumption
- VM capacity, capability, and consumption
- Intelligent, automated machine instance provisioning based on SCU^

Solutions

- Quick inventory of available resources
- Benchmarking of compute node capacity at boot
- Visibility of physical and virtual compute infrastructure for efficient operations:
  - Host compute capacity in SCU
  - VM compute capacity in SCU

Hostname	VMs	CPU	SAA Compute Units	Memory	Contention
node-9.domain.tld	5	2 CPUs × 8 cores @ 3.1GHz	7.94	9.7 GiB	17.35
node-6.domain.tld	5	2 CPUs × 8 cores @ 3.1GHz	7.94	9.7 GiB	12.97
node-11.domain.tld	4	2 CPUs × 6 cores @ 1.9GHz	3.8	7.9 GiB	10.89
node-10.domain.tld	4	2 CPUs × 8 cores @ 2.6GHz	6.47	8.6 GiB	9.67
node-7.domain.tld	2	1 CPUs × 8 cores @ 3.1GHz	4.95	7.6 GiB	7.86
node-15.domain.tld	12	2 CPUs × 8 cores @ 2.3GHz	10.19	17.8 GiB	2.73
node-16.domain.tld	0	2 CPUs × 6 cores @ 2.4GHz	2.28	3.3 GiB	0

CPI

Compute Unit

^Service Compute Unit (SCU) provides a uniform measure of capacity and consumption of compute resources

Quick Root Cause with Analytics and Remediation Engine

Pain Point

How do I prevent "blamestorming"? Is the issue my VM, host, or the cloud software?

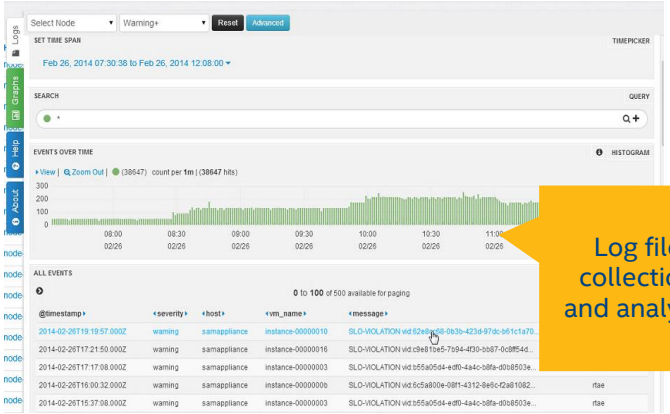
Features

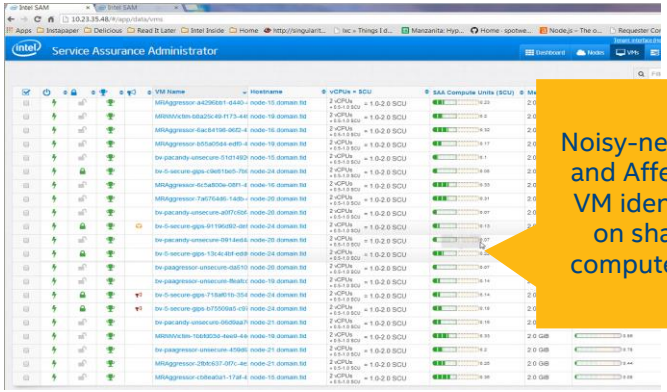
- Detects anomalies by analyzing data sources, cache monitoring, memory bandwidth monitoring, resource metrics, log file data
- Log file data collection

Solution

Administrator can use log files, graphs, charts, and alerts screens to:

- Easily identify noisy and affected VMs when service level is not being met
- Remediate performance issues once noisy neighbors and affected VMs are identified
- Get deep platform telemetry to help alleviate "blamestorming" and determine whether the physical or virtual infrastructure is in-operable



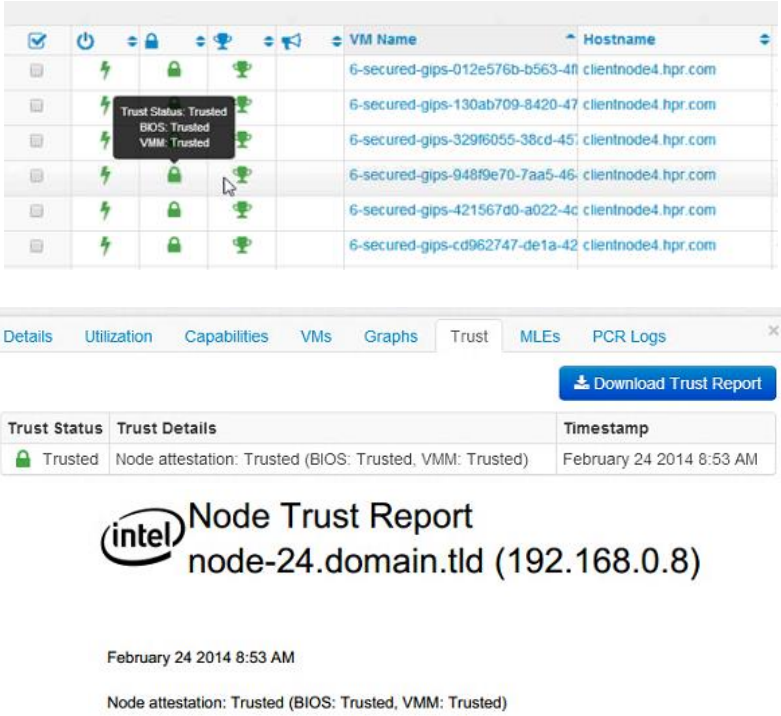


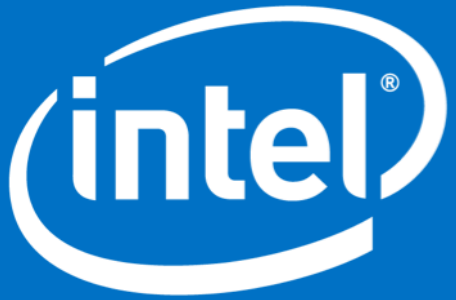
Enhanced IT Policy Compliance and Audit

Pain Point
How does IT determine that machine instances have run on trust-attested nodes and had adequate performance in their lifecycle?

Features
- Provisioning instantiation reports
- Listing of Virtual Machines instances that are running on trust-attested nodes
- Performance metrics data

Solution
Administrator uses the automated reports generated by the console to validate IT policy compliance.





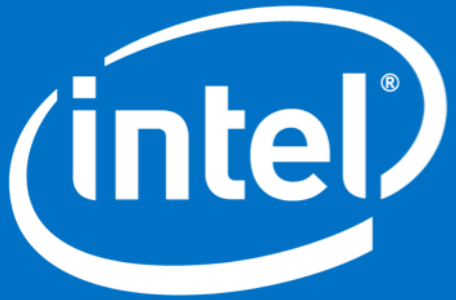
INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY 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 Product could result, directly or indirectly, in personal injury or death. SHOULD YOU PURCHASE OR USE 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.



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. Configurations: [describe config + what test used + who did testing]. For more information go to http://www.intel.com/performance

No computer system can provide absolute security. Requires an enabled Intel® processor, enabled chipset, firmware, software and may require a subscription with a capable service provider (may not be available in all countries). Intel assumes no liability for lost or stolen data and/or systems or any other damages resulting thereof. Consult your system or service provider for availability and functionality.

© 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.