PISTON OPENSTACK™ PRIMER

Piston
CLOUD COMPUTING

IF YOU'RE FAMILIAR WITH OPENSTACK® AND ANIMATED BY THE POTENTIAL OF PRIVATE CLOUD, THIS TECHNICAL BRIEF IS FOR YOU.

It will introduce you to Piston OpenStack™, Piston's turn-key software that automates the orchestration of an entire private cloud environment on commodity servers. Piston keeps your cloud running no matter what – through hardware failure, operator error, upgrades, and power outages. Delivering compute, storage, networking, and management through self-service interfaces and APIs, Piston OpenStack includes a hyper-converged hardware architecture, a highly-secure stateless Micro-OS, and advanced cluster management software.

Opinionated Software from the OpenStack Experts

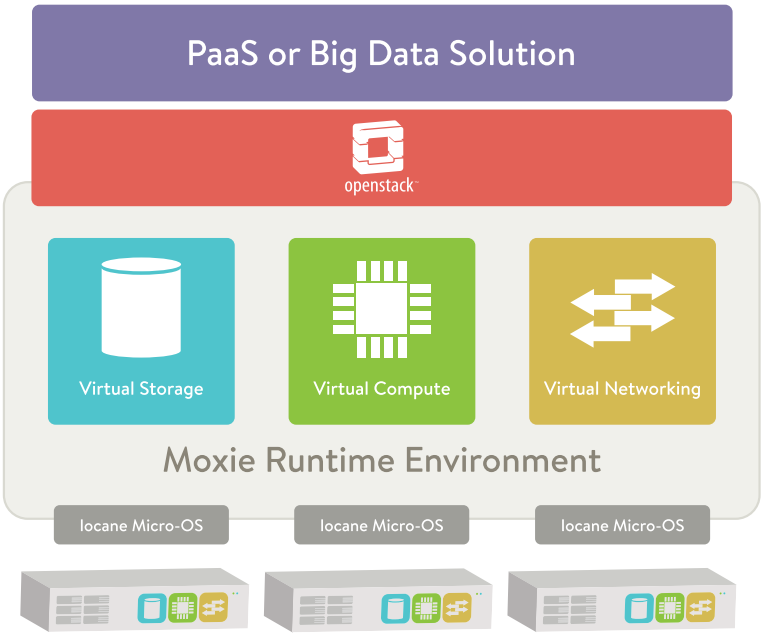
At Piston, we believe it's good to be opinionated. We won't pass

judgment on whether that combination of shirt and tie is an affront to civilized values, but we do have a lot to say about the right and not-so-right ways to architect an OpenStack cloud behind your firewall.

OpenStack is on a path to become the defining IT framework of the next 30 years. Piston OpenStack is a complete private cloud solution that delivers OpenStack that works today. So unlike many of the other OpenStack software distributions, Piston OpenStack does not focus on building on top of the OpenStack framework, but rather underneath it.

Piston OpenStack: The Easiest, Fastest, and Best Way to Run OpenStack

OpenStack is a general purpose, open source framework for cloud computing. Distinct from this generic framework, Piston OpenStack is a turn-key software product that enables enables



businesses to have an on-premise private cloud environment with little to no IT operations. Piston delivers the agility and cost savings of public cloud without the hassle of managing a typical on-premise solution. Starting with an extremely lightweight custom Linux OS called Iocane Micro-OS™, and using an advanced high-availability runtime environment called Moxie RTE™, Piston OpenStack makes it possible for a single sysadmin to manage an entire datacenter, and can be seamlessly scaled, globally, up or down. It can even orchestrate an upgrade of itself without any downtime. Piston uses a hyper-converged

architecture, that we call Null-Tier™, to deliver compute, storage, networking, and management from every single server. Piston OpenStack delivers 100% of the core OpenStack services and APIs without modification and can be deployed on your choice of commodity hardware from almost any major x86 vendor and scaled to tens of thousands of physical servers across dozens of datacenters.

With this solid foundation, we selected a limited set of curated software-defined storage, networking, and virtualization components. This allows us to ensure that the integration between these key infrastructure services is rock-solid, and also frees us to focus on making sure that the install, upgrade, scale-out, and fail-over experience for our customers is flawless. For storage, we selected Ceph™, the world's leading open source software-defined storage fabric. Piston OpenStack enables the orchestration of policy-based management of physical drives. KVM is the most popular open source hypervisor for OpenStack deployments. We have extended KVM with Virtual Memory Streaming (VMS), to support true live migration and memory oversubscription.

Piston OpenStack is built upon five pillars of value that extend the functionality and utility of generic OpenStack. This technical brief examines these pillars in turn.

FIVE PILLARS of PISTON OPENSTACK

1. **Null-Tier Architecture** - a radically simple and massively scalable hyper-converged architecture

2. **Moxie RTE** - the world's first complete runtime environment purpose-built for global-scale distributed systems

3. **Iocane Micro-OS** - a hardened, minimal Linux operating system that boots into a RAM disk

4. **Single-click update** service with zero downtime

5. **Unparalleled support** from OpenStack architects and experts

HYPER-CONVERGED NULL-TIER ARCHITECTURE:

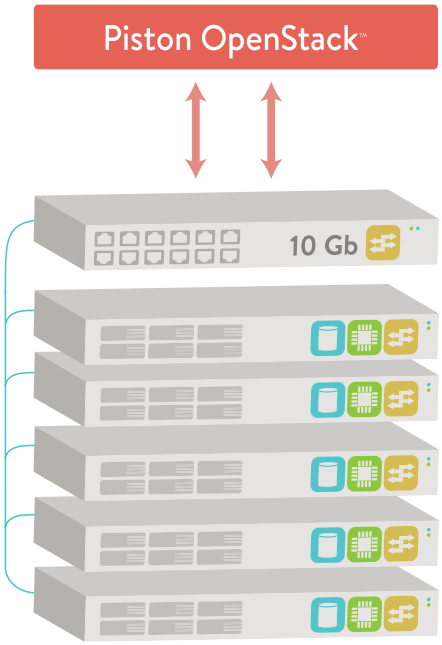
THE HEART OF THE MODERN DATACENTER

HYPER-CONVERGED NULL-TIER ARCHITECTURE:

THE HEART OF THE MODERN DATACENTER

All Piston clouds rely on a hyper-converged architecture that we call Null-Tier. This means that virtualized compute, storage, networking, and management are delivered from every single server. The evolution of technology, in every field, is a pendulum swing from special purpose to general purpose solutions. But from tractors and transport to cross-trainers and cruise ships, general purpose eventually wins out every time.

At the heart of every modern software-defined storage solution is an x86 server, with a collection of SAS, SATA, and SSD drives and a number of ethernet ports. At the heart of every hypervisor host is an x86 server, with a number of ethernet ports and a collection of drives. At the heart of every software-defined-networking controller, and every management node is also an x86 server, with ethernet and some spindles. So why not combine them?



There are countless benefits derived from a hyper-converged architecture, including:

FUNGIBILITY

As any datacenter operator can tell you, over the lifetime of

any server, the operating costs (including power, cooling, and maintenance) will be about twice the initial capital cost. And those costs are the same whether you're getting any direct value out of that server or not.

The focus on virtualization in the past decade has been a powerful driver for improving datacenter fungibility, except that it has looked only at the so-called hypervisor nodes, and ignored the wasted capacity in every management and controller node.

By embracing a hyper-converged architecture like Null-Tier, every server in your datacenter becomes fungible. The RAM, CPU cores, network bandwidth, and storage space of every single box becomes part of a shared resource pool, delivered through a single unified logical interface – the OpenStack APIs.

MAINTAINABILITY

Google was one of the pioneers of the "lights-out" datacenter model. By embracing a "next business day" support model for their hardware resources, they forced themselves to develop a distributed system's approach to infrastructure services and applications. They literally wrote the playbook on achieving resiliency in software, regardless of how unreliable the hardware underneath was. And yes, it was achieved through a hyper-converged architecture.

When individual servers aren't important, their components aren't important either, which means that a hyper-converged architecture can take advantage of single power supplies, single network cards, and cheaper commodity hard drives. The cost savings derived from using commodity servers from an entire ecosystem of vendors continue to add up.

When every node in your cluster is just dumb hardware, the only maintenance action required by a human is to power off and remove a failed node and rack a fresh one. There's no OS configuration, no "spare kit," no switch configuration, and no logging in to a CMDB and entering MAC addresses. You don't even need to turn it on.

COMBATS THE MOBILITY GAP

Most people have heard of Moore's Law by now: the prediction

of improvement in CPU performance over time.[1] Some, usually in the storage industry, have heard of Kryder's Law, a relatively equivalent improvement in storage density, and a few have heard of Nielsen's Law, which relates roughly to improvement in networking performance. But the bottom line is this: networking doesn't keep up. The gap between our ability to move data, and our ability to produce and store it, is called the "mobility gap," and it's getting dramatically worse over time.

Hyper-converged architectures such as Null-Tier are one of the only ways to combat the mobility gap.

They maximize the total bisectional bandwidth to every available spindle. A comparable traditional architecture for a private cloud might provision a single NAS filer for each rack. If these filers were provisioned with dual 40Gb NICs (and assuming the top-of-rack switch had additional 40Gb ports available), this rack of servers would have a total of 80Gb of bandwidth addressing that storage. But by using only single 10Gb NICs in each server, that same rack of servers would have a total of 210Gb of bandwidth addressing the storage fabric – almost 3 times as much.

1 *This is not technically correct. It is the density of transistors and the cost of those chips, but the derived values are equivalent.

DESTROYS OPERATOR SILOS

Cloud computing is not primarily about cost savings, it's about enabling business to go faster, to develop software at a pace that allows them to remain competitive, and to deploy and scale that software at the pace that our increasingly global market requires.

Ironically, while computers have been getting steadily faster, the delivery of IT services has been getting slower for years. This is primarily due to "silos" – the separation of IT responsibilities into networking, storage, servers, and security.

Hyper-converged architectures such as Null-Tier can tear down the walls between these silos, and allow cross-functional teams to move at the true speed of business. If DevOps is the model of agile software, then Null-Tier is the model of agile hardware.

MOXIE RUNTIME ENVIRONMENT:

TRUE CLOUD TECHNOLOGY

MOXIE RUNTIME ENVIRONMENT:

TRUE CLOUD TECHNOLOGY

Capturing the cost effectiveness of true cloud requires a hyper-converged architecture, such as Null-Tier, but in order to achieve that architecture, you also need a multi-server runtime environment. Piston OpenStack achieves this with a system called Moxie Runtime Environment (RTE), the world's first complete runtime environment purpose-built for global-scale distributed systems.

INTELLIGENT SYSTEMS MANAGEMENT

Most infrastructure services can be trivially run on every server. But some components, typically load balancers, queue servers, database servers, and other data stores, need to run a single instance at a guaranteed location. While typical configuration management approaches address this using a single "master" server configuration profile for the database, with "slave" profiles for one or more HA failover servers, Moxie RTE uses a master election approach: at runtime, any one of the nodes in your cluster is elected to operate each service. If the running process, the network connection, or the hardware in that node fails, the service is seamlessly, and automatically, re-elected to run somewhere else.

NO MORE SPLIT BRAIN

While there are a number of solutions that provide master election, what takes Moxie RTE to the next level is the way that it orchestrates "strong fencing." In order to guarantee that your cloud avoids "split brain" scenarios (where more than one node tries to operate a critical service at the same time), the Moxie RTE master election mechanism uses Zookeeper as a distributed consensus voting system. This means that if your cluster is chopped into smaller pieces by something like the failure of one or more network ports or switches, only the portion of the cluster that contains greater than 50% of the nodes can continue to "vote."

In addition, to guarantee that a node that fails catastrophically cannot hold on to storage or network resources that are required for that service, Moxie RTE will terminate the node using the out-of-band IPMI connection over a physically separate management network.

ADD & REMOVE CAPACITY WITHOUT DOWNTIME

Master election and strong fencing are already a powerful combination, but they're only the starting point; Moxie RTE also implements two separate state machines (technically, non-deterministic finite automata): one for node state and one for service state. This allows Piston OpenStack to treat the full set of dependencies between services as a state machine and orchestrate upgrades across dozens of processes and hundreds of nodes. It also manages the scale-in and scale-out processes, allowing operators of Piston OpenStack environments to add or remove capacity without a maintenance window.

THE FIRST TRULY COMPLETE RUNTIME ENVIRONMENT

Many of these technologies (master election, strong fencing, systems-level state machines) have been applied to infrastructure before, but Moxie RTE is the first time they have been combined into a complete runtime environment. The Moxie RTE Software Development Kit (SDK) allows partners and systems integrators to take advantage of this platform for any fundamental infrastructure service. For our customers, this means less time managing cloud infrastructure, and more time working on stuff that matters.

IOCANE MICRO-OS:

THE NEXT LEVEL OF SECURITY

IOCANE MICRO-OS:

NEXT LEVEL OF SECURITY

At Piston, we believe security can't be an afterthought, so we've started from the ground up with a hardened, minimal operating system that boots into a RAM disk. Iocane Micro-OS is a hardened Linux operating system, built from the upstream source. It's minimal (just a few hundred packages), which reduces the security footprint of your entire system. It's also transient. Because it boots off of the network into a RAM disk, it's never installed to a disk. So an Iocane Micro-OS upgrade is always a reboot, never a patch. When implemented properly, a micro-OS can provide many of the same security benefits as a hardware appliance without the additional lock-in.

BUILT ON LINUX

The current version of Iocane Micro-OS is built on the 3.10 Linux kernel. It provides containers, network namespaces, resource limiting and network traffic shaping to Moxie RTE. Because it can guarantee that there are no processes running in the OS that aren't managed by Moxie RTE, Piston can orchestrate otherwise destructive system functions (such as formatting and partitioning drives or powering off physical equipment) without risk.

THE NEW "RING-ZERO"

This separation of concerns between the server-level operating system (Iocane Micro-OS), and the multi-server runtime environment (Moxie RTE) is one of the key ways that Piston can use a non-deterministic, distributed systems model and produce reliable, deterministic behavior. It extends the protection ring concept of operating system design (often simplified to "kernel space" and "user space"), to encompass the reality of service-based architectures that necessarily span multiple physical machines. In cloud computing, the entire operating system should be considered "ring 0."

WHAT'S IN A NAME?

And yes, in case you were wondering, the name "Iocane" comes from the cult classic 1987 movie "The Princess Bride". In the movie, Iocane powder is an odorless, colorless, and tasteless substance. Piston's Iocane Micro-OS is an expression of that philosophy – it's a server operating system that is intended to serve transparently as a platform for running distributed services. Quite literally, it's an OS that you can't log into. And we think that's a very good thing.

SINGLE-CLICK UPDATE SERVICE

SINGLE-CLICK UPDATE SERVICE

From day one, Piston focused on making a complete turn-key private cloud software solution for companies wanting all of the goodness of an OpenStack environment, and none of the fuss of operating or managing it. In an effort to make your life even easier, your Piston OpenStack license includes access to our update service, which allows you to instantly take advantage of everything from our regular feature updates to applying security patches to your entire cloud environment with just a single click.

ZERO DOWNTIME

Clouds don't get downtime. When an upgrade is available with the latest patches, whether they are for individual OpenStack components, underlying software-defined services or the Iocane Micro-OS operating system itself, you can rest assured that it will be automatically delivered to your Piston OpenStack environment with zero downtime for your cloud. Piston's advanced systems management software enables all nodes in your cloud to be automatically updated in a rollover process without any service disruption.

Your connection to the Piston Update Service is encrypted with your unique license entitlement key. Options for updates to air-gapped installations are also available.

UNPARALLELED SUPPORT:

OPENSTACK ARCHITECTS & EXPERTS

UNPARALLELED SUPPORT FROM OPENSTACK ARCHITECTS & EXPERTS

OUR RELATIONSHIP WITH OPENSTACK

Piston is a founding Gold Member of the OpenStack Foundation, and Piston OpenStack is licensed as an official OpenStack distribution. Piston was started by co-founders of OpenStack, and we continue to provide leadership in the open source community, but we are not an open source company.

OPENSTACK – A POWERFUL FRAMEWORK, BUT NOT A PRODUCT

OpenStack is an incredible framework and set of tools for building any kind of cloud, but it is not an out-of-the-box software product. There are more than 600 configuration options in 44 separate configuration files required to get the core components of OpenStack working. The number of components and options for configuration are increasing daily.

For all of these different configuration possibilities, the time to select, test, validate, and iterate on these configurations to make them suitable for any production environment is prohibitive. It is not trivial to combine just any hypervisor with any storage backend or any number of network topologies. Without a deep understanding of these technologies and how they may or may not fit together, you can't expect live migration to work seamlessly every time without fail. Or expect floating IPs to work. Or expect your security groups to actually keep your networks isolated.

HOW WE ARE DIFFERENT

Piston OpenStack includes all of the core components of the OpenStack framework, and a curated set of virtualization drivers

for compute, storage, and networking. In addition, our Moxie RTE automates the complexity involved in configuring and managing them, enabling simple scalability and providing an incredible out-of-the-box experience.

NOT YOUR AVERAGE OPENSTACK VENDOR

Rather than shipping the latest and most recent version of OpenStack code, Piston supports each previous release until newer versions have been hardened, through further community testing and bug fixing. Typically, the OpenStack version we ship and support is 4-6 months behind the community "trunk".

While some OpenStack vendors focus on delivering the most current and "bleeding-edge" OpenStack code, we pride ourselves on delivering an amazing OpenStack experience. Therefore, we ship only the most stable and hardened version of OpenStack available, and only those components that are relevant for our customers using Piston OpenStack in production today.

About Piston

Piston Cloud Computing, Inc. is the OpenStack® orchestration company. Founded in 2011, Piston makes software that automates the orchestration of an entire private cloud environment on x86 commodity servers. Customers like Swisscom, Intelemage, Radio Free Asia, and Zymergen use Piston's secure and cost-effective AWS-like capabilities to bring new products to market faster. By managing a group of servers as a single pool of elastic and scalable computing resources, Piston OpenStack improves datacenter efficiency thereby accelerating the application development process. As an OpenStack Foundation Gold Member, Piston drives the OpenStack project forward via code contributions and thought leadership. The company is headquartered in San Francisco and funded by True Ventures, Hummer Winblad, Swisscom Ventures, Cisco Systems, Inc., Data Collective, and Divergent Ventures. Visit Piston online at pistoncloud.com.