

Understanding CloudOne's Infrastructure

The premier brand in Cloud Computing and Software as a Service for IBM® Rational®



Management Summary

As cloud computing and software-as-a-service (SaaS) are still fairly new to the majority of people in the IT world, there are undoubtedly questions as to how they are achieved in practice. CloudOne is uniquely positioned to answer questions on how to securely achieve these goals.. This whitepaper is designed to answer those questions and to provide a background for the customer or affiliate of CloudOne.

The paper is divided into three sections. The first, architecture, outlines the fundamental structure of the CloudOne environment. The second, security, addresses a fundamental question in the minds of most newcomers to cloud computing. Lastly, metrics explains how CloudOne measures and bills for it's services.

Architecture

Fundamentally, CloudOne's architecture may be understood best by seeing it as a set of distinct layers:

- Network
- Server
- Operating System
- Storage

Network

The network layer allows for the dynamic mapping of IP addresses to server clusters, as well as for secure virtual private network connections, both to users as well as server-to-server when connecting CloudOne workloads to the outside world.

It consists primarily of a fully redundant Cisco network and firewall infrastructure to deliver the highest standards of availability and security from the industry's most recognized network leader, utilizing their cutting-edge SSL VPN, split-tunneling, VLAN trunking and encapsulation capabilities, to isolate/segregate network traffic.

Server

The server layer is characterized by banks of blade-type chassis populated by Intel processor-based blade processing cards. This architecture allows both quick expansion for additional processing power, as well as the dynamic mapping of banks of processors to defined workloads.

Specifically, CloudOne uses blade servers chosen specifically to have multiple redundancy at not only the network connectivity level, but also at the power supply and cooling (fan) level. These servers offer multiply redundant hot-pluggable cooling fans and power supplies, redundant memory with failover memory banks for memory mirroring, RAID controllers for redundant storage configuration, and dual-port integrated network interface cards (NICs) with four-level network teaming for redundant network configurations.

Operating System

The operating system layer is characterized by a virtual machine hypervisor, which manages individual virtual operating

system copies running on assigned banks of blades. These virtual operating systems can be any Intel®-compatible OS, including but not limited to Linux and Microsoft® Windows®.

In particular, CloudOne uses VMWare® to implement complete virtualization of all components including servers, storage and networking allowing the management of an entire virtual infrastructure from a single point of control. CloudOne has immediate control over all customer environments and performs any necessary migrations live, with zero downtime, undetectable to users. Customer environments are also continuously and automatically optimized for performance as usage demands change.

This architecture allows CloudOne to perform all hardware maintenance without scheduling downtime and disrupting a customer's business operations.

Storage

The storage layer is defined by a large storage area network (SAN), to which additional physical drives can be added quickly, but dynamically divided into variable-size storage volumes which can be independently mapped to specific customer environments, also known as "islands" or to virtual machines. These storage volumes can also be cloned and backed up/repliated independently of operating system assistance.

Specifically, CloudOne uses this "island" environment to implement a highly virtualized storage architecture that combines intelligence and automation with fault tolerance to provide simplified administration, rapid deployment, enterprise performance and reliability, and seamless scalability. This environment is self-managing and highly scalable, and is essentially a layer that sits between connecting systems (islands) and the hardware.

Together, these four layers allow for a dynamic Cloud infrastructure, as any or all of them can be distributed across multiple data centers and mapped dynamically to customer needs on demand. In fact, by using the VMWare® technologies, we are able to move workloads from one physical data center to another without end-user awareness of the movement.

Security

With an understanding of the architecture itself, it is easier to see how high security levels are achieved. As before, viewing security as a set of layers is most helpful, which include the architectural layers as well as some additional ones:

- Data Center
- Rack
- Network
- Storage
- Blade Servers
- Virtual Machine Hypervisor
- Operating System
- Jazz Tool Server

Data Center

At the data center level, our primary facility is located in a building specifically designed for high-speed internet connectivity. It is strategically located along the I-88 "Silicon Prairie" corridor, and is connected to the Internet itself only two hops off the main SONNET ring for the Midwestern United States.

Additionally, the building itself has redundant power entry and Internet connections from different feeders on opposite ends of the building, as well as full power conditioning, uninterrupted power supply systems and redundant cooling.

Fire control is maintained with both FM200 water-less fire suppression and Fike® dry pipe pre-action fire protection systems. Access to the Data Center is controlled through key card and code access, all visitors must be escorted by data center personal at all times, and are under 24 hour video surveillance.

Access to the Data Center from outside the building is only achieved once passing a three point access process. Our data center is in compliance with ANSI / TIA 942 datacenter standards, and has completed audits for HIPAA, Sarbanes-Oxley, Gramm-Leach-Bliley and SAS-70.

Rack

At the rack level, each individual rack of equipment is under 24 hour video surveillance and is fully secured from determined or casual entry with a passlock code known only to authorized data center staff that have completed CloudOne's corporate security screening and criminal background check. The rack codes are changed at periodic monthly intervals known only to officers of the company.

Network

At the network layer, security is achieved using clientless remote access to network applications and resources, regardless of location, without the need for desktop VPN client software. Using the ubiquity of SSL encryption available in Internet browsers, the Cloud delivers clientless access to web-based applications or resources, along with terminal services access to servers for administrative purposes.

The authentication mechanism is a unified LDAP source retrieved from the customer's Active Directory instance within our infrastructure.

Storage

At the storage layer, CloudOne minimizes security risks by utilizing an isolated, non-shared "island" architecture, as well as by both physical and logical access restrictions. SAN storage is allocated by connecting a customer's "island" directly to a logical unit (LUN) storage segment, which dedicates that storage only to the customer.

As a result, only that customer can use that storage: there is no shared storage between customers. This eliminates most of the risks of the more common IT environment storage approach, including backup and restore, which are isolated only to a customer's island as well. Data access is controlled directly by the IBM Rational tools.

Blade Servers

CloudOne has standardized on blade servers in order to lower its data center footprint and improve management. We have determined that blade server products provide similar (or better) security features than racks of individual servers. In addition,

there is a physical security advantage to having the servers consolidated, and network security issues are minimized due to the integrated network components being plugged directly into (and integrated with) the blade server itself.

In addition, blades come directly from our major hardware vendor with all operating software and supporting technology (VMWare ESXi®, anti-virus, etc.) preconfigured, tested and supported directly by the vendor as an integrated system. Also, security and operational reliability is enhanced by having the OS (VMWare ESXi) installed on a memory card, eliminating any disk drives from the server blades.

Virtual Machine

At the virtual machine hypervisor level, using VMWare ESXi, the latest hypervisor architecture from VMWare, provides an ultra thin footprint with no reliance on a general-purpose OS, setting a new bar for security and reliability. The small footprint and hardware-like reliability of VMWare ESXi allows us it to also be available preinstalled on industry standard x86 servers, for rapid scalability and ramp-up.

Operating System

Operating system security is maintained using an isolated, secure, rapidly deployable, scalable Windows domain, using standard best practices for Windows Active Directory®/DNS. This AD instance is maintained as a unique container for each customer, with the ability to integrate/federate across cloud boundaries.

Tools

At the IBM Rational Jazz® tools layer, there are three security considerations.

First and foremost, all customer Jazz server instances run against authentication and on their own island, unless they are configured in a multi-tenant architecture. CloudOne's Jazz server instances access a Jazz repository with limited permissions based on unique user, group, OS, Island, and SSL VPN identity.

Secondly, a CloudOne Island has a Jazz community repository supporting the customer's community of users, with both tool and role based accesses defining read/write, update, code download and commit permissions. This "self-hosting repository" for each island's Jazz applications is a somewhat unique security configuration, and is essentially a "Secure Enterprise Repository" configuration allowing limited Internet access and integration with the island's Jazz Foundation Server web server.

Finally, we manage individual users and groups within those tool environments using a unified LDAP source for the tool environments, thereby allowing a central identity management system for each customer, with the option to possibly integrate/federate across cloud boundaries.

The most important aspect of the CloudOne security model is that every one of these layers can be integrated with a customer's security model for seamless management of the security "envelope". For example, at the user and group level, CloudOne can integrate this with a customer's own directory and role management system such that new users can be automatically provisioned as part of their larger mechanisms and strategy.

Metrics

Important to the CloudOne model is the ability to correctly assess the usage of customers in order to bill them accurately as well as to ensure that the proper number of licenses have been secured through IBM. Once again, it is helpful to see this as a set of layers that work together to achieve the cloud and software-as-a-service model:

- Peak Concurrent Users
- Measuring Peak Concurrent Users
- Billing for Peak Concurrent Users
- Provisioning from IBM

In CloudOne's peak concurrent users pricing model we align our pricing to peak user loads. This is the maximum number of users simultaneously logged in during the month, per individual application. This means that if one user logs off before another user takes their place, it is considered one, not two, simultaneous users. This might commonly occur in a workload sharing arrangement where developers from different geographical regions use a common server throughout the day and night.

In order to measure peak concurrent users, CloudOne utilizes a combination of IBM Rational's license tracking capability built into each applications "server component" and our own proprietary License Analysis Software (LAS). This data is stored in a separate, secure database, the Peak Concurrent User Data Base (PCUDB), which CloudOne's analysis, billing and reporting software accesses.

CloudOne's analysis, billing and reporting software accesses the PCUDB to generate monthly billing statements as well as high level (and detailed reports), which are available to our customers on CloudOne's help desk. Customers may view all the activity associated with each users use of any of the IBM Rational applications they are authorized to access. This comprehensive on-line access allows real time monitoring of the usage of all of a customers SaaS tools.

Furthermore, CloudOne utilizes a tier-one billing system which allows the accounting departments web access to monitor and track reporting over their lifetime. Change orders are leveraged internally, allowing customers traceability to the changes in the usage, thus generating pro-rata invoices against the specific change order. CloudOne offers a multitude of options for payment processing, paper checks on terms, pre-pay discounts, as well as recurring monthly billing are available. Industry standard security practices such as encrypted storage of sensitive data, leveraging credit card tokenization are employed in our system.

Finally, it is critical to ensure that CloudOne itself is properly provisioned with the necessary software-as-a-service licenses from IBM. CloudOne provides monthly rental, or software-as-a-service (SaaS) licenses with our pay as you go model. CloudOne controls all licensing of its SaaS software from a common set of master licensing servers which authenticate, authorize, and control each user's access to the IBM Rational applications they are authorized to use.

CloudOne's master licensing servers maintain a large pool of available IBM rational licenses from which they authorize customer's users to access the software. This complete transparency means our customers do not have to worry about licenses, but can focus on their work. CloudOne provides a report to IBM no later than the 5th of each month, based on the usage from the previous month of each customer. CloudOne provides monthly payment to IBM based on these monthly reports.

CloudOne's multi-tiered system of accurate metrics and billing is one our key capabilities, in which our customers can take comfort and confidence.

Conclusion

In short, CloudOne provides a cutting-edge architecture while employing a highly secure infrastructure and a reliable measurement methodology. You can read more about CloudOne on our website at OnCloudOne.net.

If you read this document, you will learn the following:

How CloudOne's infrastructure works, specifically in the areas of architecture, security and metrics.

For more information

To learn more about Software as a Service and Cloud Computing, as well as how they can be used to significantly improve costs and speed-to-value for development tools, contact CloudOne or one of the CloudOne Consortium business partners, or visit the following Web site: **OnCloudOne.net**



© Copyright CloudOne Corporation 2010

CloudOne Corporation
Naperville, IL U.S.A.

Produced in the United States of America
July 2010
All Rights Reserved

CloudOne and the CloudOne Logo are trademarks or registered trademarks of CloudOne Corporation in the United States, other countries, or both. IBM is a registered trademark of International Business Machines Corporation in the United States, other countries, or both. If these and other trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by CloudOne, IBM or other companies at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries.

Other product, company or service names may be trademarks or service marks of others.



Please Recycle
