Mirantis OpenStack Express: Security White Paper

Version 1.0
Introduction

While the vast majority IT professionals are now familiar with the cost-saving and agility benefits of cloud computing, many still perceive the traditional multi-tenant public cloud environments as insecure or simply incompatible with their security compliance requirements because of the lack of control they have toward the physical machines, network and storage equipment.

Mirantis OpenStack Express provides you with the ease of use of an elastic OpenStack cloud environment while providing complete controls over its underlying hardware and host operating systems configuration without compromises on security.

Because we ask our customers to trust Mirantis with their business-critical data and applications, we think it is important to describe in this paper Mirantis OpenStack Express physical and operational security measures and controls we apply in a transparent and understandable manner. We hope this will help you appraise to what extent Mirantis OpenStack Express has improved security features when compared to other more traditional, multi-tenant cloud environments.
Overview
Mirantis OpenStack Express offers on-demand private datacenters powered by the stable Mirantis OpenStack distribution running on high performance hardware that is dedicated to the sole use of your organization. It’s your private cloud.

As such, Mirantis OpenStack Express combines the best of both worlds. The elasticity and agility benefits of the pay-as-you-go cloud computing model powered by the leading open-source technology of OpenStack come along with the inherent security and privacy benefits you get from running your own private data center that is completely isolated from the other co-hosted tenants. Furthermore, Mirantis OpenStack Express is designed to be effective and easy to use. Using the OpenStack Express Datacenter Management Console, you can choose the size and characteristics of the private cloud you want and pay only for the amount of hardware you use and the time you use it. Then you can add more physical nodes (or remove them) dynamically to scale the capacity of your datacenter up and down based on the demand forecast. Once your resources are effectively provisioned in the data center, you can create one or more multi-node OpenStack highly available cloud environments using Mirantis OpenStack Fuel, the provisioning and configuration management automation engine developed by Mirantis and the community, provided out-of-the-box with Mirantis OpenStack Express.

Applied Security Measures and Controls
Physical and Operational Security
As stated above, Mirantis OpenStack Express has been design to cope with the arguably conflicting goals of providing extended controls over the data center infrastructure, including providing root access the host operating system running the cloud controller and the compute nodes (the hypervisor) while ensuring a strict isolation between tenants.

That’s the reason why the physical and operational security is the foundation of Mirantis OpenStack Express. If your data center is not physically secure, neither are the cloud environments running on top of it. No other security measures we apply at the OpenStack level would matter without it. That is why, Mirantis partners with world-class bare-metal service providers, such as SoftLayer, whose data centers are fully audited based on controls and reportings that meet industry-recognized requirements for security. This includes but is not limited to:
Data centers located only in facilities with controlled access and 24/7 security staff
- Digital security video surveillance and biometric security systems
- Machines room access strictly limited to employees and escorted contractors or visitors
- Barcode-only identification on hardware; no customer markings of any type on the machines themselves
- All data removed from re-provisioned machines with drive wipe software approved by the Department of Defense
- Engineers and technicians trained on internal industry standard policies and procedures and audited yearly
- Geographic redundancy for all core systems for disaster recovery and business continuity

Network Security
Each Mirantis OpenStack Express private data center is provisioned with two independent and isolated networks. Each physical node that is added in a private data center has two network interfaces that are bound to each network.

- One public network that is used to support egress and ingress traffic to and from the Internet
- One private network that is used to support internal traffic only

Typically, the public network is used to provide access to the OpenStack dashboard (Horizon), the OpenStack services endpoints (i.e. Nova, Keystone, Cinder, Glance, ...) and the instances public IP addresses known as floating IPs. The private network in turn is used for inter-instances communications using OpenStack Networking GRE tunneling and internal Fuel communications including PXE booting to install the host operating systems on the OpenStack controller and compute nodes as shown in the figure below.
Figure 1: Data Center Network Architecture

With Mirantis OpenStack Express, the public and private networks of your datacenter are implemented as “untagged” VLANS which means that the packets you send and receive do not contain VLAN information (i.e. 802.1Q VLAN-ID) in the Ethernet frames. For example in the figure above, customer “A” has VLAN A.1 and VLAN A.2, customer “B” has VLAN B.1 and LAN B.2 and so forth. Ports between switches and the nodes of the data center are “untagged” and so packets transmitted on your networks are just normal Ethernet packets that cannot be tampered with fake VLAN-ID information.
Data Center Management Console Secure Access

Each Mirantis OpenStack Express account is assigned a unique user id with a secure self-generated password that is protected against brute-force attacks. In addition, customer access points including the OpenStack Express Data Center Details Page, the Fuel Master Node Web UI, the OpenStack Dashboard and the OpenStack services endpoints allow secure HTTPS access so that you can establish secure communications with your cloud assets. Secure HTTPS access uses high-grade TLS 1.2 encryption based on strong and well known and standard symmetric and asymmetric algorithms like AES and RSA. Furthermore, as user with superuser privileges, you have the ability to substitute the dynamically generated certificates used in the Mirantis OpenStack environments by your own certificates signed by your Root Certificate Authority (CA).

Data Center Nodes Secure Access

By default, Mirantis OpenStack Express does not provide direct login to the physical nodes of your data center except the Fuel Master Node. From the Data Center Details page, you can obtain the SSH credentials which gives you non-root access to the Fuel Master node. Then, from there you can SSH as root to any physical node of your Mirantis OpenStack environment, including the controller node and the compute nodes, by running the command:

```
$ ssh root@node-x.domain.tld[1]
```

As root user you can change that login policy according to your own security needs and requirements.

Secure Online Payment

Mirantis OpenStack Express uses a third-party providers that are verified Level 1 PCI DSS compliant for securely storing sensitive credit cards information and for processing online payments. As such, Mirantis OpenStack Express doesn't store and even doesn't see any of sensitive information of your credit card. Instead, it is sent directly, through a highly secure connection, to a credit card vault backend and online payment service providers that will process the transaction on our behalf.

Security vulnerabilities assessment and analysis

Each release of Mirantis OpenStack Express goes through stringent vulnerability assessment and analysis both for Internet facing perimeter servers, web apps and service endpoints and from within the private data center in an attempt to identify network, server and application
vulnerabilities. Those security assessments and analysis are performed using Qualys® and Nessus® appliances. Vulnerabilities are systematically detected and fixed before a new version of Mirantis OpenStack Express is released.

**OpenStack Related Security Capabilities**

**Built-in firewalls**
Mirantis OpenStack Express brings networking services that are more flexible and powerful than security group capabilities built into the former releases of OpenStack. For example, security groups and security group rules allows administrators to specify the type of traffic and direction (ingress/egress) that is allowed to pass through a port. When a port is created in OpenStack Networking it is associated with a security group, which if not specified, is associated with a 'default' security group. By default this group will drop all ingress traffic and allow all egress. Rules can be added to this group to change its default behavior. New security groups and rules can be created by administrators, for instance, to enable HTTP and HTTPS traffic to an individual instance or group of instances.

**Role-based Authorizations and Access Controls**
The OpenStack Identity Service (Keystone) supports the notion of groups and roles. Users belong to groups and a group is assigned a list of roles. Each user can be assigned unique security credentials and roles eliminating the need for shared passwords or keys and allowing the security best practices of role separation and least privilege. Furthermore, each OpenStack service plays the role of a Policy Enforcement Point whereby a policy rule associated with each service's resource is evaluated against the user's role(s) and tenant association to determine if he/she has access to the requested resource.¹

The Identity Service along with the Policy Enforcement Points enables fine-grained access controls to the OpenStack resources. Only users with the admin role can provision new users and have access to various management functions. In turn, a user assigned to a role with lesser privileges can be confined to able to only spin up instances and attach volumes for example.

¹ Each OpenStack service has a policy file in JSON format, called `policy.json`. The policy file specifies the rules that govern access to each resource. A resource can be the service's API access point, the ability to attach a volume or to launch an instance.
Sharing Security Responsibility for Security

Because Mirantis OpenStack Express provides you root access to the physical nodes of your data center and also because you have the ability to modify the configuration of our OpenStack deployments, the security responsibilities will be shared. Mirantis OpenStack Express has secured the data center management console, the networking infrastructure, as well as the Fuel Master Node and its Web UI to provide you with fully functional cloud environments where the OpenStack security best practices are transparently applied for you. But it is your responsibility to secure anything you put on top of your cloud environment and above all make sure that custom configurations do not break the security measures Mirantis OpenStack Express has built for you. This includes the host operating systems configuration changes, the controller node and compute configuration changes, your OpenStack instances themselves and anything you install on them, any Keystone accounts that access your instances, the security group that allows outside access to your instances, the integrity of your images registry and Cinder volumes, etc.

This means that there are several security decisions you need to make and controls you must configure. For information on how to configure a particular OpenStack service, see the OpenStack Administration Guide for that service. For more tips on security best practices for OpenStack resources, see the OpenStack Security Guide. You may also want to subscribe to the OpenStack security notifications that are posted by the Vulnerability Management Team (VMT) to OpenStack Announce mailing list.