Security Overview & Data Center Certification

Operation Compliance

Abstract

Keystone Solutions is an innovative Infrastructure-as-a-Service provider

Mark Nelson / CTO

[mark@keystonesolutions.io]

Introduction

Keystone Solutions is an innovative Infrastructure-as-a-Service provider from Batesville, AR with a strong technical and business background in the hosting industry. We take pride in each customer who chooses to host with us. To us, this means they trust us with their business - everything they have at stake. Needless to say, we take this trust with the utmost importance and seriousness. We also understand that it is our task to bring transparency into the way we operate to build mutual understanding on the opportunities and responsibilities when operating in the cloud. This document is one of the ways we want to bring clarity and build trust in the way we operate our business, especially from a security point of view.

Working with Keystone Solutions

A shared responsibility model When you build your IT-infrastructure to Keystone you are entering a model where both parties, Keystone and you - are responsible to obtain the best security available. Keystone, being an Infrastructure-as-a- Service (IaaS) provider offers the technology in the physical facility where the servers are, the network connections, electricity, high-level security at the premises, networking solutions and the virtual servers as a service. Keystone also offers readily available operating system images for your virtual servers, but you may replace them with your own if you wish. What is run on the virtual servers and the applications it has been installed with, is completely the responsibility of the customer. Keystone offers and is thus also responsible for some added services such as backups made through the service and rewall configurations which the customer may use on their virtual server. However, the customer is responsible for configuring these services. In working with a sophisticated provider, such as Keystone, it is important to understand the shared responsibility model regarding your IT-infrastructure to achieve the best possible results in terms of security and performance.

Environmental security and integrity

Keystone has been built with the highest standards and requirements in mind. Our business is focused in providing our customers the best service from the best data centres around the world. We require the highest standards from the data centres we work with.

UK-LON1 - London, UK

In London, Keystone hosts its servers at a Volta facility. The data center offers approximately 8450 m2 (91000 sq ft) of floor space. It covers four floors and offers N+1 redundancy in cooling and electricity. Total cooling capacity is 8.3MW and it enjoys two separate 33kV electricity supplies from two independent grid substations. The facility has achieved the following certifications ISO9001, ISO27001, ISO14001, ISO14644-8, OHSAS 18001, PCI DSS and PAS 99.

More information on the facility is available at: https://www.voltadatacentres.com

US-CHI1 - Chicago, USA

In Chicago, Keystone works with Coresite (NYSE: COR). Their Chicago facility is located right next to the Chicago Board of Trade and thus serves customers from one of the largest financial districts in the world. The premises offer some 180 000 square feet of floor space for customer capacity. Coresite's Chicago facility offers manned security on a 24/7/365 basis including key card access, biometric scanners and video cameras. Coresite's Chicago facility is also SSAE 16 Type 2 compliant, meaning it can be used by customers in highly regulated industries such as financial services, healthcare, government, legal, biosciences, cloud computing and many others. The compliance assures CoreSite customers of the reliability of power and cooling, the security of premises and the quality of technical support.

More information on the facility is available at:

http://www.coresite.com/resources/Datasheet-Facilities-CH1

Network

Keystone treats its network with equal care and attention as it does with the other parts of its infrastructure. The network is built in a fault tolerant and resilient manner, while maintaining a high level of security. In addition, Keystone monitors its networks in all service locations on a 24/7/365 basis in multiple different ways.

All Keystone data centre facilities are connected to the API-end points in a secure and fault-tolerant manner for the provisioning of services inside the data centres. Each data centre has only access to the management servers through the API and thus do not directly communicate with any other data centre, due to Keystone's security requirements.

Designed for resiliency and redundancy - N+1 by default

One of the most important guiding design principles in all of Keystone's technology, including its network, is the resiliency and redundancy of the services in the most unexpected situations. Keystone's network architecture has been built with this in mind. We try to anticipate the most unexpected situations when we architect our infrastructure. With this principle at the core, all Keystone's data centres are connected to multiple transit connection providers. As we move inside the data centre on the networking level, all devices have been installed with the N+1 mentality in mind. If a core router, for example, breaks down, there is always at least one pair to take over its job in a matter of seconds. While this increases redundancy, it also increases the overall performance available to our customers. All networking devices follow this N+1 principle by default.

Firewall

Keystone's infrastructure firewall works in two separate stages. At the core level, we take care of the most common malicious attacks in addition to stopping DDoS-attempts.

At the second stage, the firewall is topologically located right in front of the customers' server instances. All traffic to and from the server instance always goes through the firewall first to prevent L2-level threats (such as ARP poisoning attempts) and to also further separate the server instances from each other.

The customer may also configure and use the L3-level firewall from the Keystone Control Panel or through the API. (in BETA)

Compute resources

In this section we will give an overview of the security measures used in building and designing our compute resources. The hypervisor and isolation of instances One of the most critical issues in running an environment where multiple customers share physical hardware and rely on the same software for virtualisation is the isolation of instances in a secure and thorough manner. Keystone relies on KVM due to its strong guest isolation procedures. Because KVM is built into Linux, the KVM guest processes are subjective to the same principles that a Linux operating system follows regarding its user process separation. Despite the continuous development of separation processes, the most basic separation mechanisms have existed since the beginning and have thus undergone thorough testing and certification.

KVM’s Type 1 design is similar to other x86 hypervisors, such as VMWare and Xen. KVM further uses virtualisation specific processor instructions to ensure isolation of guests from the hypervisor and from each other. A third level of isolation and protection is added by Intel’s virtual machine extensions (VMX) and AMD Secure Virtual Machine (SVM) instructions. KVM is an open source initiative and is thus continuously inspected and tested for flaws by a wide community of users.

Host operating system

Those Keystone personnel with a need to access the host operating system for administrative purposes do so through specially defined procedures. In addition to unique credentials to dentify all users, all user activity is logged.

Guest operating system

The guest operating system is the software deployed by the customer onto the virtualised server. Keystone’s personnel have no access to the guest operating systems whatsoever. In ther words Keystone has similar capabilities as anyone else attempting to access the server from the public internet. Thus it is extremely important that you configure your server security in such a way that you are able to access it at all times.

Storage resources

In addition to the compute resources (CPU and memory) a core part of the service are the storage resources Keystone offers. In this part we go over how we have designed the services from a security point of view and what this means for the customer. Storage backends - HDD & MaxIOPS Keystone offers two types of storage backends to its customers, HDD and MaxIOPS. here is no distinction in how these storage systems have been produced regarding security. because the storage backends utilise Infiniband based fabric, it is not possible to access the storage systems from the public internet. To further build redundancy to the storage backend, Keystone always keeps all customer data on two separate storage backends in the same data centre. On both storage backends the data is further RAID- secured. This is a standard procedure for all disks deployed and used on Keystone.

Backups

Customers are also able to set scheduled backups to further increase security and redundancy. Backups on Keystone are handled on a third, separate storage backend from the live production data in the same data centre. Therefore if a loss of data occurs in the production environment, the backed up data is not affected in any way.

Scrubbing deleted disks

Once customers delete their disks on Keystone, the disk enters a process where Keystone thoroughly writes the disk with non-meaningful data to clean it completely for new use. This process is commonly called scrubbing and it is a standard procedure applied to all disks that are deleted from customers' servers on Keystone, be it through the control panel or the API.

API access (in Beta)

Connections to the Keystone API access point always proceed through SSL-secured connections. Authentication takes place through the HTTP Basic access method using a unique username and password. By default, the API connection credentials are not available for newly registered accounts and the customer must create account specific credentials through the Keystone control Panel. It is also possible to limit API access further by source IP-address.

Control Panel (in Beta)

All connections to Keystone control panel are passed over SSL / HTTPS. Users need to have a valid functioning username and password to enter the Control Panel. In the case of a lost password, users need to retrieve it with access to both the e-mail and telephone number used during the registration process.

Data Center Certification & Operations Compliance

More information on the facility Compliance is available at:

http://www.coresite.com/data-centers/data-center-design/compliance