SECURITY in the RACKSPACE® CLOUD

An overview of our best practices

Table of Contents

1. INTRODUCTION 3

2. GENERAL SECURITY 5

2.1. Spheres of Responsibility 5

2.2. Physical Security 6

2.3. Network Security 7

2.4. Data Security 8

2.5. Business Continuity and Incident Management 12

2.6. Compliance and Regulation 13

3. SERVICE-SPECIFIC SECURITY 14

3.1. Cloud Servers™ 14

3.2. Cloud Files™ 17

3.3. RackConnect™ 18

1. INTRODUCTION

VIEWS OF "SECURITY" WITHIN CLOUD COMPUTING

As a shared-tenancy hosted environment, cloud computing raises a number of inherent questions around its security. Rackspace® Hosting has engaged hundreds of customers about this issue and we found at least one common theme: when customers talk about "security in the cloud" it means different things to different people.

It is clear that across the industry cloud providers and their customers share concerns around the data itself, as well as network security, account and access control, compliance and regulations. Additionally, the spheres of responsibility between the service provider and the customer are not always clear.

This document addresses these areas within the context of the Rackspace Cloud. We have found our customers appreciate thinking about this massive issue in the buckets highlighted in Figure 1.

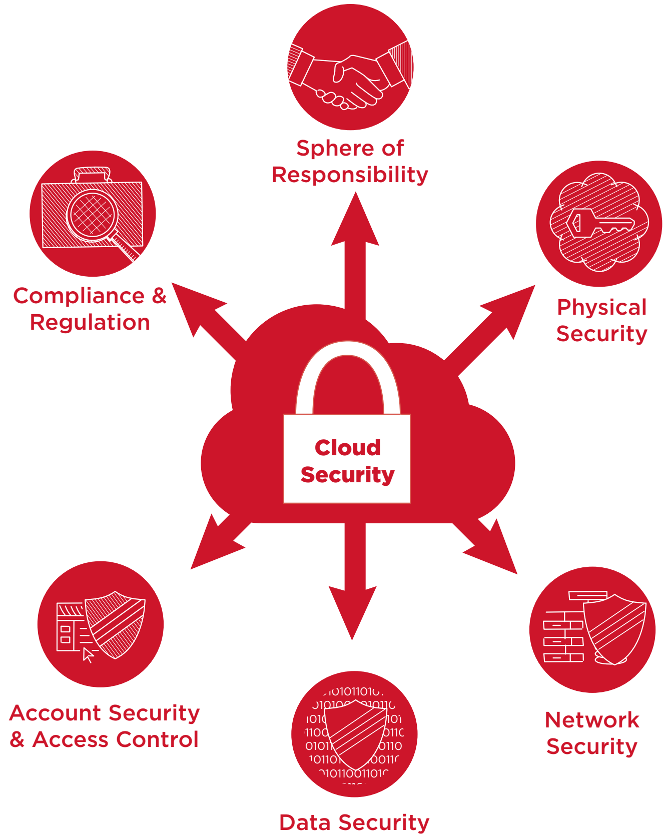

Figure 1: Security in the cloud

Spheres of Responsibility: Given the role of the customer in the configuration and consumption of their cloud environment, both the cloud provider and cloud customer must accept responsibility for different aspects of the system and both must implement a range of controls in order to properly secure the service. This whitepaper will detail the different aspects that must be managed for overall security in the cloud, specifically what should be addressed by the provider and what is the responsibility of the customer.

Physical Security: Cloud providers have a responsibility for the physical security of their data centers and the cloud infrastructure hosted within them. In this section, we will detail the different physical security measures that Rackspace has implemented to secure its data centers.

Data Security: Data security in the cloud begins with the identification and assessment of the unique risks faced by the data that the customer wishes to host in a cloud environment. Rackspace has implemented controls to manage the risk of compromise to our internal networks and via the hardware and hypervisor layers and can also provide services and guidance on addressing those risks identified by the customer. As the data owner and the primary system administrator of their cloud solution, the customer is ultimately responsible for data security issues.

Account Security and Access Control: Account security and access control are key areas of concern in any outsourced hosting solution and no more so than with cloud based services. Customers require that only authorized users maintain access to their solution and that accountability is maintained. Rackspace has put in place appropriate safeguards to tightly restrict access to our back-end infrastructure and can recommend services to assist the customer in efforts to enforce account security and access controls above the hypervisor layer.

Compliance and Regulation: Rackspace maintains an internal security management system to ensure that it meets the requirements of applicable legal and regulatory obligations. It is the customer's responsibility to comply with relevant laws and regulations that impacts their data hosted in the cloud.

It is important to note that many of our best practices are applicable across our entire portfolio of services (e.g. data center security), whether dedicated hosting or cloud. Where applicable, we have inserted specific Cloud Servers™ and/or Cloud Files™ detail into this framework. Additional product specific detail for Cloud Servers, Cloud Files and RackConnect™ is included at the end of the document.

2. GENERAL SECURITY

2.1. SPHERES OF RESPONSIBILITY

Characteristics of Multi-Tenancy

Given the shared hardware nature of any public cloud environment, it is vital that both the cloud provider and cloud customer put controls in place to manage the risks presented by multi-tenant environments. Rackspace utilizes a range of infrastructure level measures to protect customer solutions and ensure the segregation of customer footprints for those areas within our sphere of responsibility and control. These should be complemented by controls implemented by the customer in response to the specific risks applicable to their hosted data.

Rackspace

Rackspace maintains control of the physical security of the hosted solution and the configuration of the shared Rackspace infrastructure including hypervisors and the management networks, as well as any Rackspace-owned APIs.

Customers

Customers are responsible for protecting the confidentiality of their Rackspace Cloud API keys, temporary API tokens and account credentials. Rackspace customers are expected to employ appropriate safeguards to protect the information stored in their cloud environment. Customers can regenerate API keys on-demand to help ensure that their API access is not compromised.

In addition, cloud Servers customers are responsible for disabling non-essential remote root logins. Customers are responsible for performing all server-level actions and maintenance, including installing patches for the OS and application stack. Our cloud Servers with a Managed Service Level offering (or “Managed Cloud Servers”) provides an option whereby Rackspace employees act as your system administrator in the cloud and patch and update Operating Systems and various applications.

Rackspace recommends that customers configure a software firewall (e.g. iptables or Windows Firewall) on newly created Cloud Servers instances so that both the public and private interfaces are protected by suitable controls. Customers are also encouraged to harden new servers immediately according to best practices.

2.2. PHYSICAL SECURITY

Data Centers

Rackspace Cloud services are currently available in three of the eight Rackspace data centers. Rackspace data center physical security capabilities include:

- Two-factor authentication required to access all data center facilities.
- Electromechanical locks controlled by biometric authentication (hand geometry or fingerprint scanner) and key-card/badge.
- Access to secure sub-areas allocated on a role-specific basis.
- Only authorized data center personnel have access to data halls.
- Authorized Rackspace personnel's access to the facilities is reviewed on a monthly basis by management.
- Termination and role-change control procedures are in place so that any physical or logical access rights are removed in a timely manner when access is no longer necessary or appropriate.
- Closed-circuit video surveillance is installed at all entrance points on the interior and exterior of the buildings that house data centers. Cameras are monitored 24x7x365 by on-site security personnel and support data retention for 90 days.
- Sensitive equipment such as information processing facilities, including customer servers, is housed in secure sub-areas within each data center's secure perimeter and is subject to additional controls.
- Centralized Security Management Systems are deployed at all data centers to control the Electronic Access Control Systems and closed circuit television networks.

Rackspace data centers are operational 24x7x365 and are manned around-the-clock by a security team and engineering/operations personnel. Appropriate additional perimeter defense measures, such as walls, fencing, gates and anti-vehicle controls are in place at Rackspace data centers. The delivery and loading bays at all Rackspace data centers are separate areas secured by defined procedures and security controls.

Unauthorized visitors are not permitted access to the data centers. Authorized data center visitors are required to abide by the following rules:

- Authorized approvers must specifically grant visitor access to the data centers at least 24 hours before the scheduled visit.
- Visitors must have a valid reason for entering the data center.
- Visitors must sign the visitor's log, present a valid photo ID, and specify the reason for visiting and a Rackspace point of contact.
- Visitor badges differ in appearance from Rackspace employee badges and do not provide any control over doors, locks, etc.
- All visitor access is logged. This policy applies equally to Rackspace employees not assigned to the data center.
- Visitors, including Rackspace customers, are strictly forbidden from accessing the data halls themselves and other secure sub areas.
- Visitors must be escorted at all times while at any Rackspace facility.
- Data center management performs a monthly audit of security and visitor access logs.

2.3. NETWORK SECURITY

A secure cloud service must be supported by strong network security measures gathered from an effective risk assessment. While the requirements for conventional network security are still applicable, Rackspace has implemented additional steps tailored to manage the risks posed by web-scale virtualization and the scope of our cloud environments. Rackspace can provide services and guidance to assist with the management of additional risks posed by the customer's operational model.

Access to Network Services and Devices

All Rackspace network infrastructure devices are located in a physically secure data center with controlled access. All visitors or authorized contractors are logged and escorted. Local console access to network devices is restricted to authorized individuals and requires access to the physical location as well as the correct username and password for console login. While Rackspace utilizes a wireless infrastructure for corporate connectivity, wireless access points are not permitted in the data halls where the cloud infrastructure resides and regular scans are performed to identify and neutralize rogue access points.

Administrative access to the networking devices underlying the cloud infrastructure is controlled via industry standard practices (TACACS+) and is subject to appropriate logging and monitoring, records of which are retained for one year. Logical access to cloud infrastructure network devices is only provided to those Rackspace employees with a strong business requirement for such access and is subject to permissions change control including independent managerial authorization and timely revocation of access rights. Administrative access to network devices is encrypted.

Provisioning and Configuration Management

Provisioning of new cloud environments is performed according to standardized procedures in order to minimize the risk of accidental insecure network provisioning. Changes to existing cloud network infrastructure are controlled by formal change management processes to reduce the risk of accidental insecure configuration.

Policies on the Use of Network Services

Rackspace maintains strict policies on the use of network services. The network services underlying our cloud infrastructure are subject to DDoS/DoS mitigation and network policy enforcement controls, ensuring the best possible quality of connection to the customer's cloud resources and maximizing the stability of the environment at large. These include anti-spoofing controls and IP prefix-lists, as well as Unicast Reverse Path Forwarding (URPF) protocols in place at edge routers in data centers hosting cloud environments. Further environment specific measures such as automatically provisioned hypervisor controls are in place to control the malicious or accidental misuse of network services by the cloud resources themselves.

24x7 network operations teams continually monitor bandwidth statistics and network traffic trends for anomalies suggesting inbound DoS/DDoS attacks. Appropriate action including the null routing of involved IP addresses for the duration of the attack is taken to mitigate the infrastructure level impact of any DoS/DDoS targeted at cloud resources.

2.4. DATA SECURITY

Data Security Policy and Foundations

Cloud security depends on the clear identification and management of data security risks generic to all IT services, both outsourced and in-house, as well as those unique to massively virtualized and cloud-based environments. While Rackspace recognizes its responsibility for the management of the subset of these risks where we can exercise control, the customer should manage the security of their hosted data due to the level of freedom and control potentially exercised by the customer and structure of the services themselves.

Rackspace believes that good cloud security begins with a strong risk assessment on the part of the customer. Not all data is well-suited to a public cloud environment and the strength of risk management controls should match the requirements of the customer's data protection obligations. Rackspace provides a Cloud Readiness Assessment to assess the suitability of moving existing applications and create a concrete recommendation for cloud adoption. As part of the Cloud Readiness Assessment, Rackspace will evaluate applications (for performance, security, architecture, integration and risk) in your environment that are candidates for migration, and suggest risk mitigation strategies.

Following a risk assessment, customers should implement an appropriate security policy and identify suitable controls to remedy the identified risks. This will ensure that the measures put in place by the customer complement the controls maintained by the provider to arrive at a comprehensive and coherent security system.

Rackspace maintains control over the physical and network security of the infrastructure supporting cloud services (typically up to the virtualization layer) and over Rackspace administrative access to the infrastructure. Rackspace provides comprehensive support up to the virtualization layer and has implemented appropriate infrastructure controls, as we consider all customers hosted data to be of the highest sensitivity.

In addition, Rackspace has employed appropriate controls to manage risks to customer cloud services stemming from vulnerabilities in the shared infrastructure.

Rackspace Operational Procedures and Responsibilities

Rackspace maintains documented operational procedures for both infrastructure operations and customer-facing support functions. Newly provisioned infrastructure undergoes appropriate testing procedures to limit exposure to any hardware failure. Documented procedures and configuration version controls provide protection from errors during configuration. Changes to an existing shared infrastructure are controlled by a technical change management policy, which strictly enforces best practice change management controls including impact/risk assessment, Change Approval Board sign off, and back-out planning. Staging environments are used by QA and change control teams to test infrastructure changes, fully highlight risks, and are entirely segregated from the production environments. Internal testing data is only used for testing purposes.

Shared Infrastructure Communications and Monitoring and Hardening

Administrative communication with the Rackspace Cloud back-end infrastructure operates over encrypted channels. Infrastructure devices sit on a dedicated management network.

Infrastructure devices are provisioned with hardened base operating systems, which are subject to appropriate patch management activities, further reducing the surface attack presented by infrastructure middleware. Rackspace maintains close ties with our Hypervisor vendors and critical updates and patches are applied. Elements of the infrastructure critical to service delivery, such as critical logistics devices, physical hosts, and storage nodes are actively monitored for health and availability and any system alerts are rapidly responded to by a geographically distributed 24/7 available operations team.

The public cloud is only provided with API mediated access to infrastructure functions and devices, ensuring that only a restricted and appropriate command set is available subject to key based authentication and authorization. Customer facing APIs are provided via SSL enabled endpoints providing customers with an encrypted and verifiable channel to issue API requests. Customers should verify all SSL certificates being presented by API endpoints.

Infrastructure Level Customer Segregation Controls

A key concern in public cloud environments is the level of segregation between customer resources and the assurances that a cloud vendor can provide.

The Rackspace Cloud Servers environment enforces physical segregation of customer images and data at the storage layer via the use of a Virtual Hard Disk (VHD) file system. Customer data is maintained in a virtual hard-drive space by the VHD system and is only exposed to the correct server. VHDs are presented to the Cloud Server as a physical resource, and the server will only be aware of and able to access the correct VHD. The resources underlying the VHD are exclusively reserved for that instance from creation until eventual destruction. Processes within the hypervisor abstract customer's Cloud Servers from other physical resources such as CPUs and memory and enforce segregation. The hypervisor also maintains automatically provisioned logical and virtual network controls to enforce separation between customer traffic and to provide network security policies at the infrastructure and hypervisor layers. Hypervisor level networking controls should be complemented by actions within the customer's sphere of responsibility in order to secure their traffic at higher layers.

Rackspace Cloud Files enforces customer segregation via the environment's logistics and authentication systems. As a massive array of redundant storage, the physical storage location and management of data within the Cloud Files environment is administered by "logistics" servers. A location and account mapping for each file is maintained, and the account tokens supplied by the authentication servers are required before the logistics server will serve up any given file. The logistics servers mediate all public communication and no other public connectivity to the storage arrays is maintained.

Rackspace Employee Access Controls and Operational Safeguards

All Rackspace employees are provided with unique usernames and passwords, and administrative access to cloud environments is tightly restricted to those employees with a strong business requirement. Cloud infrastructure access is allocated on a role specific basis, and privileged infrastructure access is tightly restricted to the Operations team, who are subject to comprehensive background screening. Cloud customer support administrators are only provisioned with access above the virtualization layer and to customer cloud resources as appropriate to their role. Access to cloud infrastructure devices occurs over encrypted channels and requires the user's unique cryptographically strong key. Access to the cloud infrastructure is terminated upon employee termination or change of role, and access keys are audited and refreshed on a quarterly basis to remove inappropriate accounts. Moreover, access to cloud management systems is controlled with multi-factor authentication, detailed transaction-level logging, and network-based access restrictions.

Data Redundancy – Cloud Servers and Cloud Files

Rackspace Cloud services provide a level of resiliency at an infrastructure level, and provide customers with the availability of their data though snapshot functionality.

The physical drives supporting the file structures underlying Cloud Servers are provisioned in a RAID 10 arrangement providing a base physical level of redundancy. Storage resources are allocated to a Cloud Server during build and are reserved for that Cloud Server until it is ultimately destroyed, providing data persistence for paused or deactivated Servers. Customers are able to snapshot operational Cloud Servers and store the image automatically in the Cloud Files environment, and may use these snapshots as images to build new servers.

Cloud Files is eventually consistent massively distributed file storage architecture. The Cloud Files infrastructure automatically replicates uploaded data across three 'zones' within a given data center which are physically separated and served by fully redundant data center services. Zones are served by redundant utilities and power. Maintenance processes replicate any changes to the data across the copies, maintaining consistency.

Data Destruction – Cloud Servers and Cloud Files

Cloud Servers instances themselves maintain no logical access to physical storage resources or disk sectors. Therefore, the data is rendered effectively unrecoverable from the instance after a server instance is deleted via control panel or API. Latent data from previous cloud server instances cannot be read from new instances that are launched on the same hypervisor.

Deletion of data from the Cloud Files environment via control panel or API removes the file entry from the file table. As the files are stored on a distributed massive storage array with zero non-API or proxy mediated network access, the files are therefore effectively undiscoverable and unrecoverable by a public connection. Requests for deletion of local files are stateful and a success or fail result will be returned for every action. Where files have been distributed to the Akamai network by enabling CDN distribution, Cloud Files also supports edge purge functionality to clear the files from the CDN provider's edge distribution nodes. CDN edge purges are asynchronous and purge assurance can be tracked via the automated success/failure email alerts. Customers are limited to a maximum number of CDN purges a day. Whole container purges are only available through support ticket.

Failed Physical Drives

Any surplus or failed physical drives from the cloud environments are sanitized before being returned to inventory. Failed drives that are within warranty are degaussed. Drives that reach an "end of life" state are physically destroyed.

Recommended Customer Controls

Rackspace infrastructure controls are designed to protect cloud resources from attack within the environment appropriately control and provide assurance over Rackspace access to customer cloud resources. The customer should seek to protect their cloud resources and hosted data with measures overlaying Rackspace infrastructure controls as appropriate to their data's sensitivity and criticality as informed by a formal risk assessment.

Customers are the primary owner of their Cloud Files hosted data and maintain sole visibility over its specific security requirements. Accordingly, customers are responsible for classifying their data and applying appropriate risk mitigation controls. Customer's sensitive data should be encrypted for storage in order to preserve confidentiality. Rackspace recommends that data being transmitted to and from the cloud should be subject to encryption appropriate to its requirements, for example the use of TLS or a secure VPN. Rackspace can provide SSL certificates through partner contacts and VPN-based products like RackConnect to assist with the security of data in transit.

Rackspace Cloud customers interact with the environment at an administrative level via API and console access and must authenticate using persistent API or keys. Account level authentication credentials provide access to large-scale commands such as Cloud Server creation, deletion and re-sizing and Cloud Files data CDN enablement and should be protected by commensurate organizational and technical controls. Customer applications that interface with Rackspace Cloud APIs should undergo adequate security testing and maintain best practice application security controls including communication with our SSL protected API endpoints via HTTPS. Customers should consider tightly restricting access to API keys and account credentials to those employees with a legitimate business requirement, as well as segregating duties to maintain accountability. Customer's root level Cloud Server credentials should be subject to similarly strong internal safeguards. Customers may reset their Cloud Server's root password (or administrative password).

Customers have particular responsibilities when consuming Cloud Servers services, having full access to log into their servers remotely using secure shell (SSH) or Windows Remote Desktop. (Platform dependent) Rackspace customers are allowed to make changes to their servers as needed and Rackspace recommends that the customer harden their Cloud Servers by appropriately configuring software and security settings, restricting operating processes and services to those required, including removing or securing default accounts and passwords. Customers should seek to implement cohesive versioning controls and patching policies for operating systems and applications in order to minimize risk stemming from un-patched vulnerabilities and replicated Cloud Server images. Customers are also advised to maintain appropriate security services on any Cloud Server including up to date and well configured software firewalls on all public and private virtual network connections and regularly updated anti-virus capabilities.

As primary system administrator of the cloud resources, the customer is responsible for managing user accounts creation, provisioning and destruction, password policies, server level account authentication mechanisms, etc. Rackspace recommends that customers integrate their Cloud Servers resources with their organizational Single-sign on (SSO) domain if available in order to simplify this task.

2.5. BUSINESS CONTINUITY AND INCIDENT MANAGEMENT

Rackspace is committed to a Business Continuity Program that helps us meet service levels agreements (SLAs) reflected in customer contract language. Our Business Continuity efforts are consistent and reflect industry best practices. Business Continuity at Rackspace involves ensuring that supporting internal applications, utilities, and network infrastructure remain operational after any service interruption event.

Specific highlights of the program include:

- Redundant utility (data, voice, electric) providers and supporting SLAs
- Highly redundant '100% uptime' shared network architecture
- Adequate inventories for hardware failure replacement
- Backup generators and electrical controls at each data centre capable
- Remote support sites for customer contact support
- Backups of corporate support applications
- Periodic data center infrastructure restoration and contingency testing

Explicitly, the Rackspace Business Continuity Program does not include customer specific cloud resources or customer data hosted in the cloud. The customer should consider their Recovery Time Objective and Recovery Point Objectives when transferring data to cloud services, and structure their overall solution to satisfy these requirements.

Rackspace maintains formal incident response processes concerning both corporate network incidents and incidents affecting customer solutions. Incidents that affect more than one customer or Rackspace operations (Enterprise Impacting) are managed from a centralized tool that provides alerting and escalation paths and procedures, communication procedures and command, control and communication across all Rackspace facilities. Rackspace will alert the customer to incidents impacting their cloud solution at the data center and infrastructure levels in a timely fashion, but due to the potentially dynamic nature of cloud service utilization Rackspace does not perform proactive monitoring of customer's specific cloud resources. Should the customer require that Rackspace provide additional monitoring and incident management capabilities over and above the shared infrastructure the customer should consider the Managed Cloud product offering.

2.6. COMPLIANCE AND REGULATION

SSAE 16 / ISAE 3402 (formerly SAS70 Type II)

SSAE 16 and ISAE 3402 are the new international service organization-reporting standards. In the US, the AICPA (American Institute of Certified Public Accountants) created the Statement for Standards for Attestation Engagements (SSAE) No 16 to mirror the ISAE 3402. The SSAE 16 and ISAE 3402 Type II SOC 1 audit and report supersedes and effectively replaces the Statement on Auditing Standards (SAS) No. 70 Type II. Rackspace recognizes the needs of our International and US customers and has worked with the service auditor to have the report issued with a joint opinion that satisfies the requirements of both the ISAE 3402 and the SSAE 16. The new report, ISAE 3402 / SSAE 16 Type II SOC 1 is available to our customers and prospects.

Safe Harbor

With respect to our Safe Harbor certification: You can find more information about what is covered under our certification at **https://safeharbor.export.gov/list.aspx**. You'll also find our self-certification addresses what data we collect and how we process such data. When providing information technology hosting services, Rackspace may process personal data controlled by its customers. Rackspace processes that data at the direction of its customers and in accordance with the terms of its agreements with its customers and a data processing agreement in place with each of its entities located in the EU.

ISO 27001

Rackspace has received certification of the ISO/IEC 27001:2005 Information Security Management System (ISMS) Standard for select data centers. The standard was created by the International Organization for Standardization (ISO) and is governed with the International Electro technical Commission (IEC).

ISO/IEC 27001:2005 is the formal international security standard against which organizations may seek independent certification of their Information Security Management System (ISMS). It is intended to be used with ISO 27002:2005, a Security Code of Practice.

Customer Responsibility

The customer owns the business processes that ensure that the cloud hosting infrastructure meets the data security components of internal policies (for example, IT security policy), or any regulatory or industry compliance requirements (for example, PCI-DSS).

3. SERVICE-SPECIFIC SECURITY

3.1. CLOUD SERVERS™

Hypervisor

Rackspace Cloud Servers is a multi-tenant public cloud environment utilizing Xen-based hypervisors and a set of proprietary logistics and middleware nodes, offering both Linux and Microsoft Windows guest Operating System (OS) images. Customers may interact with their guest instances through the control panel or via the RESTful Application Programming Interface (API). Both methods enable customers to retain full control over your Cloud Server configuration. Rackspace implements controls for the physical security and environmental resilience of the underlying hardware, including network connectivity, and the management and maintenance of the shared infrastructure up to the hypervisor level. While Rackspace provides industry-leading levels of support around the underlying infrastructure, customers are considered the primary system administrators and are ultimately responsible for the configuration and maintenance of their Cloud Server instances, unless utilizing our Managed Cloud product as referenced previously.

Data Redundancy

As Cloud Servers are given pre-allocated physical storage resources upon creation, Rackspace is able to provide data persistence whether your Cloud Server is in an active state or shut down. Physical drive arrays are in a Redundant Array of Independent Disks (RAID) 10 configuration, providing a measure of data redundancy. Customers are able to snapshot Cloud Servers images and upload them to their Cloud Files account. Rackspace recommends that customers perform regular snapshots of their Cloud Servers to provide for better availability of data and processing facilities. The snapshots can also be used to create new identical instances to provide scalability or further redundancy.

While Rackspace cannot guarantee that each of a customer's Cloud Server is located on separate physical resources, the logistics algorithms underlying the creation of new customer Cloud Servers is designed to heavily favor the separation of an individual customer's machines. Rackspace does not support a multi-data center or geographic redundancy of the Cloud Servers product at this time.

The Cloud Files environment automatically enforces the replication of hosted data. On initial upload, the Cloud Files environment replicates an incoming file across multiple separate zones in the data center. The zones are supplied with redundant utilities and connectivity. The infrastructure enabling the Cloud Files product is fully redundant, and the hash tables containing the location of uploaded files are distributed over all storage and proxy nodes. Like Cloud Servers, Cloud Files does not currently support multi-data or geographic redundancy of data.

Network

Within the Cloud Servers product, newly created instances are configured with two network interfaces by default. The front, or public, facing interface is allocated a unique IP address that is used to route traffic from the instance to the Internet. A secondary interface is allocated and assigned an IP address that is not routable to the Internet and is used for communication between instances in the same data center and with other Rackspace services.

Customer segregation in Cloud Servers is enforced by the hypervisor. Hypervisor controls are in place to prevent MAC, ARP and IP spoofing on the public and private virtual interfaces of each Cloud Server. If a malicious user attempts to spoof IP or MAC addresses, those specific malformed packets are discarded. These rule sets prevent a given Cloud Server from sniffing the traffic of another, even one hosted on the same physical resources. Logical network security is the responsibility of the customer.

Guest Isolation

Segregation of physical resources such as memory, hard-drive space and CPU usage is also enforced by hypervisor controls. Each Cloud Server is allocated a volume when it is created and each server is aware of only the storage assigned to it. The Cloud Servers hypervisors are only accessible to Rackspace and only via on the private management network and require appropriate administrative SSH keys.

Access

Access to the instance is provided by the username and password returned to the user upon instance creation. For Linux instances, pre-generated SSH keys can be passed in with the initial request over the API. The service adds these keys to the instance and grants the user access over SSH. Customers can regenerate API key on-demand so that their API access is not compromised. For more information about account security and access control, including authentication and API keys, see the **Data Security section**.

Cloud Server Instance Deletion

When a customer deletes an instance, the instance is turned off and stored for as long as the instance has been in use, or 12 hours, whichever is shorter. After this interval, the instance is then scheduled for deletion from the system and the instance data is consequently rendered unrecoverable from the hypervisor's disk. This retention period allows administrators to recover instances that were deleted by accident within a reasonable timeframe. After the retention period, latent data from previous Cloud Server instances cannot be read from new instances that are launched on the same hypervisor. For more details, see **Data destruction – Cloud Servers and Cloud Files**.

Managed Cloud Differences

Managed Cloud instances provide Rackspace administrator access. The password for this account is rotated on a set schedule by Rackspace management systems. When a Rackspace administrator accesses this data, it is logged and the password for the account is rotated.

RackConnect™ Differences

Cloud Servers that are part of a RackConnect configuration contain a RackConnect user that is built in to provide the RackConnect system access to manage network and software firewall settings, which are part of the RackConnect solution. This is an administrative account, but the credentials are not accessible by Rackspace administrators, only by the RackConnect automation system. Essentially, it is a system or service account. The password for this account is rotated on a set schedule by Rackspace management systems. Access and use of this account is logged, just as with the "rack" user for managed cloud instances.

Images

Rackspace encourages customers to make routine backups of their Cloud Servers environments. These backups can be done by making a copy of the current server image and placing it on Cloud Files. As these images could contain sensitive information, it is important for customers to ensure that only authorized personnel have access to the Cloud Files buckets containing the images.

Control Plane

As part of our support process, Rackspace routinely accesses the hypervisors providing the various cloud services. This access is enabled using a management network internal to the Rackspace data centers that are not accessible from outside our networks. This access is only used for management purposes and is restricted to a pre-defined set of Rackspace employees and tools.

Customer Responsibility and Best Practices

Rackspace is responsible for the Cloud Server up through the hypervisor level. Customers have full administrative access to their cloud environments and they are considered to be the system administrators responsible for the upkeep of the system including maintaining compliance with their internal security or operational policies.

In general, Rackspace recommends that customers include a host-based firewall in their configuration, such as IPTables or the Windows Firewall. The firewall should be configured with a default deny policy and only necessary ports should be enabled for access. Both the public and private network interfaces should be protected. In addition to firewalls, Rackspace recommends that customers maintain a regular patch policy so that the server operating system and applications are updated regularly with their respective security patches.

3.2. CLOUD FILES™

Rackspace Cloud Files offers scalable, utility-billed file storage accessible via control panel, API and third-party applications. The Cloud Files environment automatically replicates uploaded customer data across multiple zones within a single data center, served by redundant power and networking utilities.

Cloud Files is an object storage solution, and does not implement encryption, virus detection, or compression on objects entering and/or exiting the system. Many of these functions are available through third-party tools, but they are ultimately the responsibility of the customer, not the Cloud Files system. Customers can monitor their data activity via logs that can be automatically delivered to their account.

Customer Segregation

Cloud Files enforces customer segregation via the environment's proxy and authentication systems. As a massive array of redundant storage, the actual location and management of data within the Cloud Files environment requires administrative activity by the proxy servers. A location and account for each file is maintained, and the appropriate tokens supplied by the authentication servers are required before the proxy will serve up any given file.

3.3. RACKCONNECT™

Hybrid Cloud Hosting

Using RackConnect, a customer's dedicated and cloud-hosted solutions can communicate directly over an internal network. RackConnect can blend hosted private cloud as well as the Rackspace Cloud with dedicated hosted infrastructure, based on the needs of each customer, creating a flexible and extensible hosting platform that can be customized and scaled quickly as needs change. RackConnect leverages a dedicated network appliance to manage traffic between dedicated and cloud. This network appliance, either a firewall or load balancer, is not solely dedicated to RackConnect – it can continue to function as needed as part of the customer's hosting solution as well. Cloud Servers that are integrated within a RackConnect solution a hybrid solution can take advantage of the customer's dedicated firewall and other security products, such as Intrusion Detection Systems, DDoS mitigation, and Web Application Firewalls to help guard against external threats. Customers configure Network Security Policies in the MyRackspace® portal, and these policies are then used to automatically update and maintain access rules on both the RackConnect network device as well as the software host-based firewalls on cloud servers, further enhancing the security of the entire solution. This architecture creates a very flexible infrastructure, capable of greatly enhancing the security controls possible in a cloud deployment.

Network Security

RackConnect requires the dedicated customer solution to use a compatible network appliance (examples include a Cisco ASA firewall, F5 Big IP Local Traffic Manager, or a Brocade ADX load balancer). Communication between cloud and dedicated servers occurs between a Cloud Servers internal virtual network interface and a specific physical interface on the customer's firewall or load balancer. With RackConnect, customers can configure a range of network policies in the MyRackspace customer portal, defining access restrictions and rules that define the hosts and protocols allowed to communicate within their configuration, as well as between internal hosts and the Internet. These policies are then applied automatically by the RackConnect solution at the appropriate locations in the network.

Policies governing communication between cloud and dedicated servers are applied as packet filters or access control lists (depending on the network appliance in use). Polices defining cloud server communication within the cloud, or between cloud and the Internet are applied to the host-based firewall on the Cloud Servers themselves, access control lists (firewall) or packet filters (F5) to implement the defined network security policy. These controls are further enhanced by the hypervisor controls in place that enforce message routing and help prevent IP/MAC spoofing. Note that when deploying RackConnect, Rackspace must manage the customer's network appliance that is used. This device can still exist in an managed colocation configuration, but the customer does not maintain administrative access to this particular device after RackConnect is deployed.

RackConnect Network Policies allow a customer to define source and destination for all desired traffic within their solution, and this policy is maintained for them. This Policy is set in the MyRackspace customer portal, and can be set very generally, such as allowing all servers within a customer's environment to communicate on all ports with all other servers, or using very specifically, specifying only specific hosts, ports and protocols to be allowed.

As new Cloud Servers are added to an account, the Network Policy is automatically applied at build time, leveraging the IPTables software firewall on Linux-based servers, or Windows Advanced Firewall rules on Windows servers; in addition, packet filters are added to the RackConnect network appliance. The other existing Cloud Servers in the customer's account are then also updated, so they can communicate with the newly added server.

When a Cloud Server is deleted, rules are removed from the RackConnect network appliance, as well as the IPTables or Windows Firewall rules on all of the remaining Cloud Servers in the customer's account. Furthermore, rule sets on the host-based firewalls are also verified and reset as needed on a regular basis for compliance with the customer's defined network policy. This automation is important in maintaining the security posture of the customer's infrastructure. Since the cloud can be a very dynamic environment – in fact, it is designed to be so – maintaining host-based security can be a very manual and painstaking process. The larger the environment, the more administrative overhead involved. By defining Network Policies at the account level, RackConnect helps that policy is automatically and consistently applied, even in the most dynamic of infrastructures. Automation helps eliminate manual errors as well as security policy is maintained in all cases, even when a system administrator is in a hurry.

VPN Access

RackConnect also can be used in conjunction with a VPN connection from a customer site (office network or another data center). A Cisco ASA is used to terminate a site-to-site IPSec or SSL VPN, with one tunnel end at the customer site, and the other within the customer's dedicated hosting environment at Rackspace. This creates a secure, encrypted tunnel for traffic that traverses the public Internet. This capability allows a customer to extend their own data center or network infrastructure over the Internet; to include Rackspace hosted servers and infrastructure, whether that is dedicated hosting, hosted private cloud, or Rackspace Cloud.

DISCLAIMER

This Whitepaper is for informational purposes only and is provided “AS IS.” The information set forth in this document is intended as a guide and not as a step-by-step process, and does not represent an assessment of any specific compliance with laws or regulations or constitute advice. We strongly recommend that you engage additional expertise in order to further evaluate applicable requirements for your specific environment.

RACKSPACE MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, AS TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS DOCUMENT AND RESERVES THE RIGHT TO MAKE CHANGES TO SPECIFICATIONS AND PRODUCT/SERVICES DESCRIPTION AT ANY TIME WITHOUT NOTICE. RACKSPACE RESERVES THE RIGHT TO DISCONTINUE OR MAKE CHANGES TO ITS SERVICES OFFERINGS AT ANY TIME WITHOUT NOTICE. USERS MUST TAKE FULL RESPONSIBILITY FOR APPLICATION OF ANY SERVICES AND/OR PROCESSES MENTIONED HEREIN. EXCEPT AS SET FORTH IN RACKSPACE GENERAL TERMS AND CONDITIONS, CLOUD TERMS OF SERVICE AND/OR OTHER AGREEMENT YOU SIGN WITH RACKSPACE, RACKSPACE ASSUMES NO LIABILITY WHATSOEVER, AND DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO ITS SERVICES INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT.

Except as expressly provided in any written license agreement from Rackspace, the furnishing of this document does not give you any license to patents, trademarks, copyrights, or other intellectual property.

Rackspace, Rackspace logo, Fanatical Support, MyRackspace, RackConnect and/or other Rackspace marks mentioned in this document are either registered service marks or service marks of Rackspace US, Inc. in the United States and/or other countries.

All other product names and trademarks used in this document are for identification purposes only to refer to either the entities claiming the marks and names or their products, and are properties of their respective owners. We do not intend our use or display of other companies’ trade names, trademarks, or service marks to imply a relationship with, or endorsement or sponsorship of us by, these other companies.