TECHNICAL OVERVIEW

# SERVICE DELIVERY ENVIRONMENT ACCESS METHODS: RACKSPACE PRIVATE CLOUD OPENSTACK

rackspace®

AUGUST 16, 2018

# TABLE OF CONTENTS

# INTRODUCTION

In the course of providing Fanatical Support® to your OpenStack Private Cloud Environment, Rackspace will, from time to time, need to access your environment. We know how imperative it is to your business that we maintain secure, audited and restricted access.

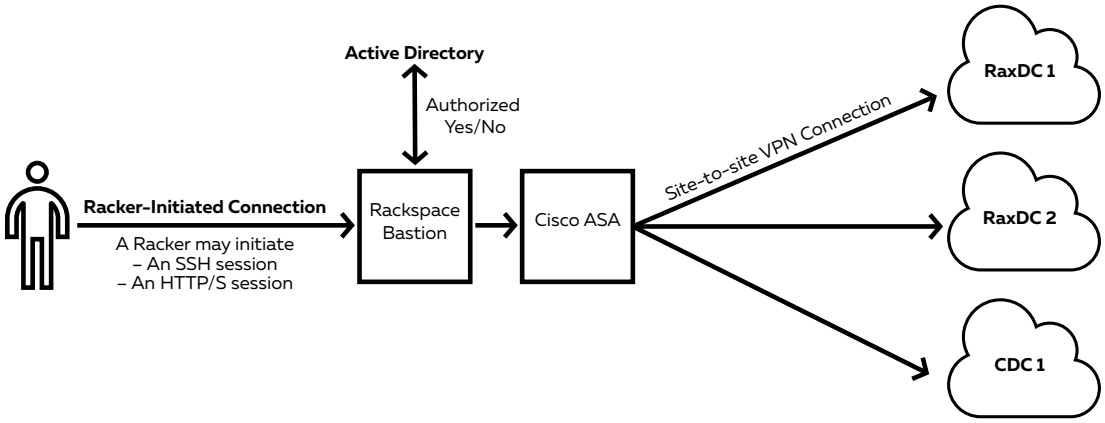
Because of this need, we have put controls in place so that our support engineers can never directly access an environment from their desktop. This process provides you with assurance and traceability of "who" is doing "exactly what" in your environment at all times.

# HOW DO WE CONTROL ACCESS?

All service delivery traffic must traverse through a Rackspace bastion server solution whose sole functionality is to control and monitor administrative protocols used for remote access or management to your environment. The bastion is hardened to ensure that standard passwords, user accounts, unneeded services and daemons are permanently disabled to significantly reduce vulnerabilities from potential attackers.

The bastion server's control and audit-tracking capability are designed to satisfy the following:

1. Only approved personnel can access the environment.
   a. This is controlled via Rackspace Active Directory/LDAP groups and permissions.
   b. No group access, password rotation rules or identities are stored on the bastion server. The bastion server uses Active Directory exclusively.
   c. Logging into the bastion server is strictly controlled with SSH public and private keys stored in the Active Directory metadata for a given user to ensure that access revocation is immediate.
2. All actions by Rackspace personnel are recorded through audit logs, and the logs can be provided upon request for a nominal fee.
   a. Audit trails are session recordings that are triggered by a Rackspace Service Delivery Engineer initiating a connection to the bastion server to access the environment.
   b. Audit trails are indexed on the bastion server, but can also be externally indexed for further performance considerations. In the case of large amounts of audit trails (i.e., high concurrent connection count/per day), external indexing spreads the load to reduce load on the Balabit device itself so it won't get bogged down.
   c. In addition to the audit trails above, the system logs for the bastion server are also stored and securely sent to a log aggregation system (syslog-ng/etc.) to provide additional system logs that contain audit data.
3. The bastion servers themselves do not contain sensitive data except for the audit logs. Site-to-site VPN connectivity, for example, is handled directly on the firewalls in front of the bastion servers.




**Standard Rackspace Connectivity**

## WHAT IF I HAVE GREATER SECURITY OR COMPLIANCE NEEDS?

Compliance requirements or other security restrictions may require you to purchase a dedicated bastion server implementation. In this scenario, we follow similar procedures as with the standard deployment. A Rackspace Service Delivery Engineer will still initiate a connection via SSH, HTTPS or RDP as required to perform debugging and/or maintenance tasks for your environment(s).

The connection request is then routed through a fully patched and secured firewall that has a site-to-site VPN to your environment's firewall. This means any and all traffic is encrypted and secured.

By opting to have a dedicated bastion server, all service delivery traffic is exclusive to your environment.

This means:

1. Compliance and security auditors will have the assurance that there is no traffic traversing the device that is not intended for your environment.

2. Your own set of audit trail information, the dedicated server, will ensure that you can access the audit data and replay it to confirm or review as required.

3. The configuration of your dedicated bastion server will match the configuration of the Rackspace bastion server to ensure consistency.

## WHAT CAN WE ACCESS?

Upon accessing your environment, the scope of what our Rackspace Service Engineers can perform is limited to the data center.

The scope of actions the Rackspace Service Delivery Engineers will take is restricted to supported control plane nodes, compute nodes and storage nodes to troubleshoot and resolve infrastructure issues. We will also access the underlying infrastructure in the environment to perform firmware upgrades (if Rackspace maintained), operating system patches and upgrades, logs and configuration file reviews and enhancements to the Rackspace-provided Operational Tooling Fabric.

Rackspace does not log into, access, troubleshoot or support the customer's virtual machines (instances).

If these methods do not meet your compliance/security requirements or you would like a different access method or a more hardened environment, it will require a discussion with our Professional Services team to appropriately identify how Rackspace can accommodate your requirements.

We understand that providing a highly secured, validated and audited access system is required to gain your trust and confidence. We believe the solutions we offer will give you faith in our abilities to operate your private cloud with the reassurance of being able to audit what we are doing.

# ABOUT RACKSPACE

Rackspace is the #1 provider of IT as a service, in today's multi-cloud world. We deliver certified expertise and integrated managed services across public and private clouds, managed hosting and enterprise applications. Because Rackspace partners with the leading technology providers, including Alibaba®, AWS, Google, Microsoft®, OpenStack®, Oracle®, SAP® and VMware®, we are uniquely positioned to provide unbiased advice on the technologies that will best serve each customer's specific needs. Rackspace was named a leader in the 2017 Gartner Magic Quadrant for Public Cloud Infrastructure Managed Service Providers, Worldwide and has been honored by Fortune, Glassdoor and others as one of the best places to work. Based in San Antonio, Texas, Rackspace serves more than 150,000 business customers, including a majority of the Fortune 100, from data centers on five continents.

Learn more at www.rackspace.com or call us at **1-800-961-2888**.



AUGUST 16, 2018

PRI-WTD-RPC_OpenStack_Technical_Overview-12196

rackspace®