Rackspace Configuration Monitoring

What is it?

Rackspace has partnered with UpGuard (https://www.UpGuard.com/) to provide instrumentation for configuration discovery, change monitoring and policy checking on selected customer devices.

This facility enables us to scan a device periodically to determine what software and versions are installed, how the operating system and installed applications are configured and what services are running. A record of historic scans is maintained which enables an administrator to quickly determine:

- How a device configuration has evolved over time
- How one device configuration differs from another
- How devices differ from the ideal state as defined in a policy

Why do I need it?

A large proportion of incidents are due to a change, rather than hardware failure which one can engineer around to a large extent. A recognition of this fact is embodied in the disciplines of Change and Release Management which seek to contain and mitigate the risks implicit in rolling out changes through increased rigour with regards to:

- Risk evaluation
- Planning
- Review
- Scheduling
- Documentation

A Change Manager would seek to maintain a full record of all changes committed within his/her area of oversight. If all changes followed the established process, all changes were executed with no deviation from the plan and the planned steps always resulted in the expected end state, the Change Manager's system of record would be complete.

Unfortunately, there are many opportunities for changes to deviate from the expected. During an incident, the answers to the following ostensibly simple questions may be frustratingly elusive:

- What has changed since this last worked?
- Who changed it?
- Is this server configured like all the others in the same role?
- Do our devices run vulnerable software version x?
- Is our DR environment a faithful replica of production?

There is no surer way to gain this clarity than through empirical observation. By directly observing the configuration on mission critical infrastructure, we can empower our customers to answer these questions quickly and with certainty.

Combined with a Change Management process, Rackspace Configuration Monitoring can help to provide assurances that the outcome of a change was true to the intent and that unapproved changes are captured and can be policed.

Rackspace Ltd

5 Millington Road, Hyde Park Hayes, Middlesex, UB3 4AZ
http://rackspace.co.uk/

How is this Achieved?

- Agentless install – discovery is via SSH and WinRM connections.
- Virtual appliances within the customer's solution (connection managers) and a Rackspace managed configuration item (CI) repository which also hosts the WebUI. The discovered data does not leave the Rackspace perimeter and is accessible only to Rackspace and the customer themselves where they have subscribed to this service. An existing VMware footprint in the customer solution is required for this deployment model; alternatives can be discussed on a case by case basis.
- The set of devices to be monitored is agreed and remote connectivity from the UpGuard appliances is configured in line with the agreed Change process.
- Once initial discovery is successfully performed, Rackspace and the customer will work together to appropriately group devices and develop policies to be applied to these groups.

What is Delivered?

Initial Setup

Service Setup and Initial Configuration

In this initial phase Rackspace will install the necessary components, such as connection manager appliances, and configure the target nodes and the UpGuard appliance for discovery. Rackspace will then need to work with the customer to agree and create the credentials required for discovery. Changes may be required on the target nodes themselves: enabling the winrm listener on Windows hosts; creating a local discovery user and adding a public key to .ssh/authorized_keys for this user on Linux hosts. Firewall changes may also be required to enable network communications. Rackspace will then be able to proceed with the addition of the subscribed nodes and configure a scanning schedule.

Secondary Configuration

Once the service is able to successfully scan all of the customer's subscribed nodes, we'll work with the customer to ensure that they are appropriately grouped, typically by role. The policies Rackspace will then help the customer create will operate on these groups to enforce consistency across the associated groups.

Once the policies are in place, it is possible that some inconsistencies will be discovered with the first subsequent scan. Rackspace will work with the customer to remediate these where they are consequential to the correct functioning of the groups or tune these out of the policies where they are not. With these initial defects out of the way a baseline would have been established.

Periodic

Daily Emails

Once users are signed up to the appliance, they will begin to receive daily emails from the appliance providing a brief summary of policy failures, detected changes and discovery failures. Detailed reports will be available via the appliance on a self-service basis.

Monthly Change Report

While the customer will be able to draw their own reports via the appliance as needed, Rackspace will present Change Reports monthly to coincide with the regular Service Review. Rackspace are working to support a higher automated report cadence for those who prefer delivery via email.

Rackspace Ltd
5 Millington Road, Hyde Park Hayes, Middlesex, UB3 4AZ
http://rackspace.co.uk/

Ongoing/Continuous

Incident Response

Where an Incident occurs involving a node covered by this service, Rackspace Support and Customer operations staff will be able to quickly determine what, if anything, changed since the last known good state.

Notifications

These will consist of the daily summary emails from the scanner, contact from Rackspace in response to policy violations which require attention and, in future, optional scheduled reports delivered via email.

UI Access

Customers will have ongoing access to the WebUI for self-service.

The Service

The Hosting Services Agreement (HSA) for this service will contain the following description for the subscription:

"Rackspace Configuration Monitoring via UpGuard

- Rackspace Configuration Monitoring via UpGuard is sold to you as an Unsupported Service and, for the avoidance of doubt, service level agreement(s) does not apply to the service.
- Support for Rackspace Configuration Monitoring via Upguard will be provided during 08:00 GMT to 18:00 GMT Monday to Friday on a reasonable endeavours basis and shall include:
  - Configuration discovery for nodes
  - Nodes and Policy scans once every 24 hours
  - Node group and policy creation assistance
  - Responding to policy violations and escalating to you
  - Monthly Change Report
- Any support from UpGuard must be directed to Rackspace only.
- You will be charged for Rackspace Configuration Monitoring via UpGuard on a monthly basis based on the number of units ordered. For the avoidance of doubt, you will be charged for the service for the whole month even if the server to which the service is applied to is deactivated for all or part of that month."

Along with the subscription, for which the customer stipulates node coverage, the customer will have access to the WebUI, the API and the full suite of UpGuard capabilities on a self-service basis for those nodes covered by the subscription. The customer is supported and advised by Rackspace, underpinned by UpGuard.

Please note: No changes to the existing agreed SLAs or other service commitments are implicit in the subscription agreement.

Rackspace Ltd
5 Millington Road, Hyde Park Hayes, Middlesex, UB3 4AZ
http://rackspace.co.uk/

Feature Availability for Subscribed Nodes			
Feature	**Description**	**Rackspace Support**	**Customer Self-service**
Configuration difference	For the nodes in scope, determine what has changed since last known good as a part of Incident response	X	X
Configuration discovery	Discover configurations for scanned nodes. Tailor scans to specific roles as necessary based on consultation between Rackspace and the customer	X	X
Configuration monitoring	Monitor configuration changes on discovered devices. Retain change history for a minimum of 3 months where scan intervals are no smaller than 24 hours	X	X
Configuration discovery data security	Discovery data is retained local to the UpGuard appliance within the customer's solution. Backups of this data may be retained on the Rackspace Managed Backup service where this is already agreed and in place for the customer. Information derived from discovered configurations may be exported via the Web UI or UpGuard API in the form of reports for Rackspace and customer consumption. Where a change of architecture may be required (e.g. to facilitate scaling), no changes will be performed without the agreement of the customer.	X	X
Initial Defects report	In order to baseline the configured node groups prior to policy institution and enforcement, an initial group diff is performed to detect inconsistencies between devices performing the same role. Action, either an approval of the defects or approval of a plan to remediate these defects, is required prior to policy institution	X	X
Device groups	Rackspace will work with the customer to implement device groups which correspond to node roles (for the purposes of policy enforcement) or application boundaries	X	X
Notification for policy and change events	Customer contacts can be configured for the receipt of notifications whether these be daily change reports or policy violation reports.	X	X
Policy configuration	Rackspace will work with the customer to implement relevant policies for each device role where these roles are represented by a device group.	X	X
Policy enforcement	Police consistency across groups of devices	X	X
Policy notification response	Rackspace will respond to notifications on policy violations and escalate to the customer as necessary. The customer is expected to respond to such escalations in order to a) mitigate any resultant risk and b) ensure policies remain current and relevant	X	X
Reporting (Monthly)	Monthly Change report delivered by Rackspace	X	
Scanning appliances	UpGuard virtual appliance and connection manager provided free of charge to customer with the customer providing compute and storage from their VMware infrastructure	X	X
CSTAR risk assessment	Generate CSTAR risk assessments per node (self service via UI). https://www.upguard.com/cstar		X
Customer WebUI access	Customer has full access to the UI to perform self service activities such as: generation of ad hoc reports, generation and updating of policies, the performance of ad hoc scans, etc.		X
DevOps enablement	Customer may generate base recipes/manifests/configs from discovered configurations.		X
Reporting (ad hoc)	Ad hoc reports on change and policy compliance may be drawn on a self- service basis via the UpGuards UI or API.		X

Rackspace Ltd
5 Millington Road, Hyde Park Hayes, Middlesex, UB3 4AZ
http://rackspace.co.uk/

Pricing

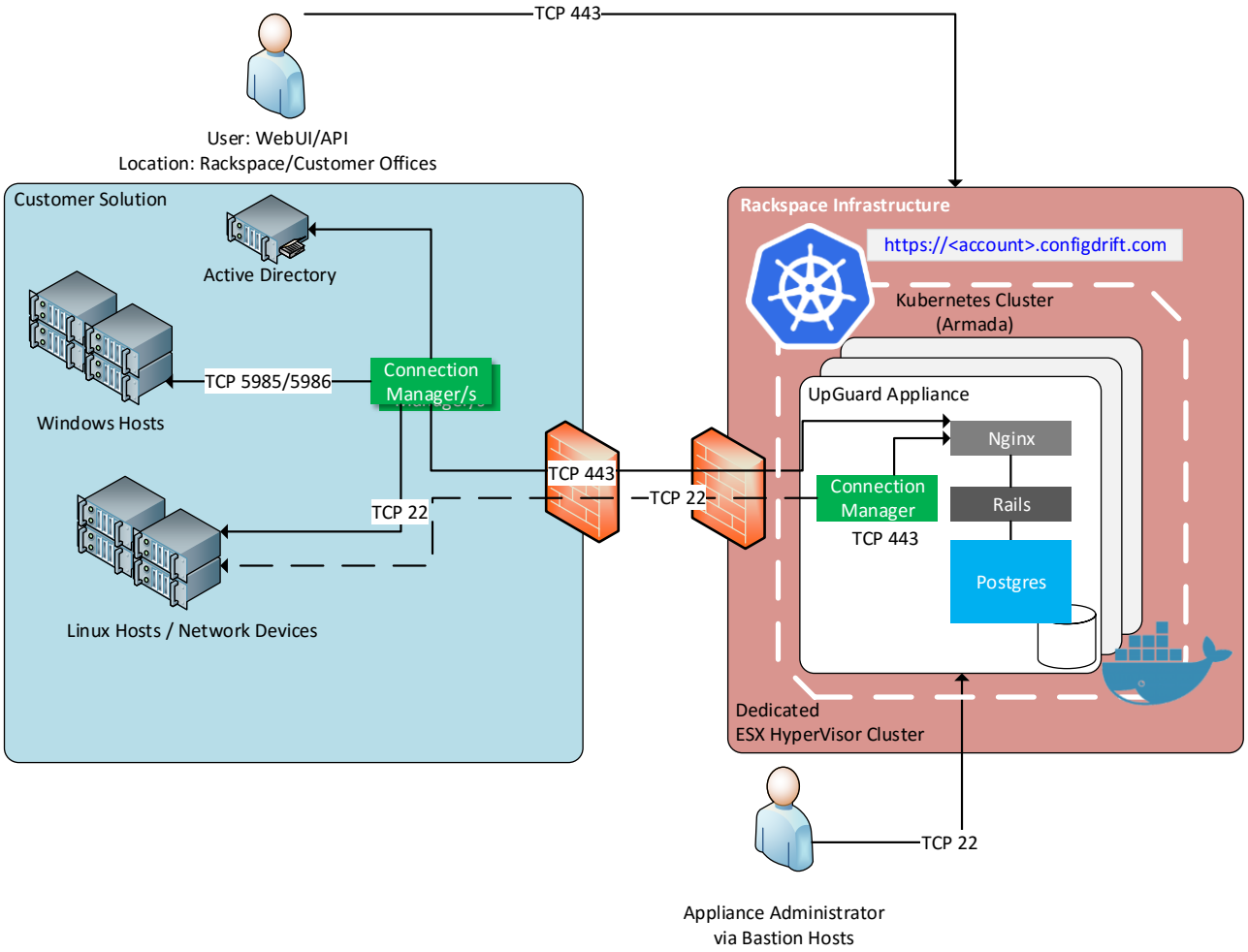
Pricing is per node monitored per month:

Currency	Amount
GBP	11.50
USD	14
EUR	13.80
AUD	20.50

The Setup Fee is calculated at 1 months MRR, per node per deployment. For example, if a customer purchases licensing for 5 nodes in GPB, the setup fee would be £10 per node, multipled by 5 nodes totalling £50.00 Setup Fee.

Rackspace Ltd
5 Millington Road, Hyde Park Hayes, Middlesex, UB3 4AZ
http://rackspace.co.uk/

Architecture



Next Steps

Should you wish to learn more, a walkthrough of the basic features of this product will be arranged by your Service Delivery Team. In that session we'll be interested to understand what node(s) you are considering, the pain points you are most keen to address with this enhanced visibility and how we can best facilitate this and with whom in your organisation we would be working with in order to achieve this.

Rackspace Ltd
5 Millington Road, Hyde Park Hayes, Middlesex, UB3 4AZ
http://rackspace.co.uk/