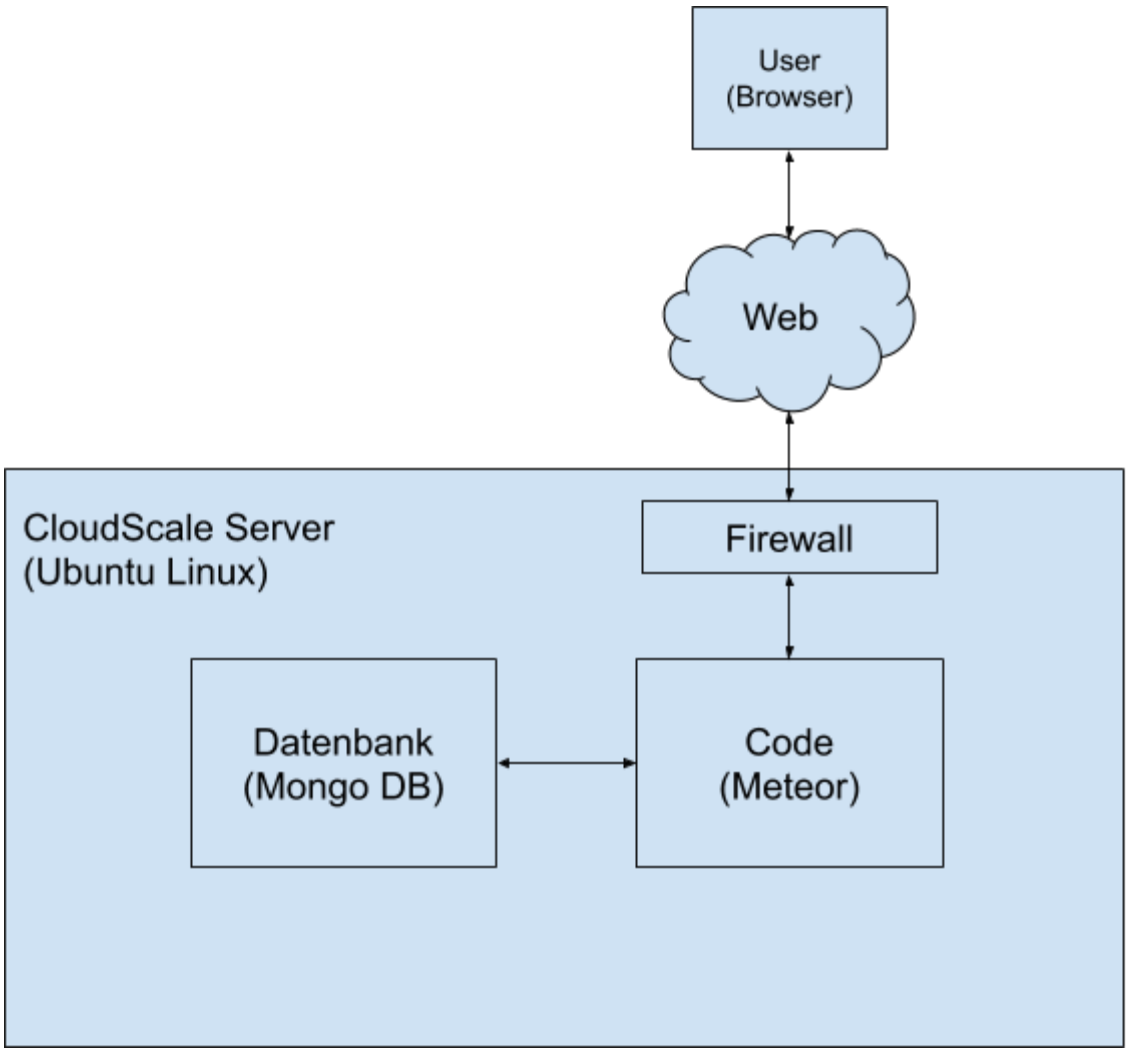
joineer

Zusammenfassung der IT Architektur

IT Architekurzeichnung

Die Infrastruktur der cloudscale.ch AG ist bei der e-shelter Dataschutz AG in Rümlang, Zürich in der Schweiz untergebracht.



Die Datenbank und der Code aller Joineer Produkte befinden sich auf dem Server von Cloudscale.

Im folgenden wird auf die wichtigsten Punkte der Serverinfrastrukur von Cloudscale eingegangen:

Physische Separierung

cloudscale.ch verfügt über ein eigenes sog. Cage, d.h. ein separater, abgeschlossener Bereich innerhalb des Rechenzentrums, in welchem nur Racks von uns stehen und Dritte keinen Zutritt haben. Der Vertrag für dieses Cage wurde auf 5 Jahre (mit der Option zur Verlängerung um weitere 5 Jahre) abgeschlossen, um die physische Sicherheit langfristig auf höchstem Niveau gewährleisten zu können.

Stromzufuhr und -redundanz

In dieses Cage wird auf zwei verschiedenen Trassees Strom von unterschiedlichen Unterverteilungen, welche wiederum an unterschiedlichen Hauptverteilungen angeschlossen sind, auf zwei verschiedene Stromschienen pro Rack geführt. Beide Hauptverteilungen werden bei einem Stromausfall von separaten USV-Clustern gestützt bis einer der Dieselgeneratoren (2N+1 Redundanz) die Last übernimmt. Beide Hauptverteilungen sind je im Ring an unterschiedliche Zulieferer (EWZ und EKZ) angeschlossen. Die Redundanz wird vom RZ-Betreiber in regelmässigen Abständen getestet (sog. Autark-Tests).
Alle unsere Systeme sind an beide Stromkreise angeschlossen, so dass wir den Ausfall eines Netzteils - oder eines ganzen Stromkreises - ohne spürbare Auswirkungen auf den Betrieb verkraften können.

Klimatisierung

Die Rechenzentrumsfläche ist frei von wasserführenden Leitungen und wird von einer sog. Klimaspange (Umluftkühlgeräte: 2N Redundanz) umgeben. Das Wasser wird in einem Ring geführt, so dass bei einem Defekt einzelne Abschnitte unterbrochen und repariert werden können, ohne dass dadurch die Zuleitung zu den restlichen Umluftkühlgeräten gefährdet wäre. Das Gebäude verfügt zudem über eine Free-Cooling-Anlage auf dem Dach. D.h. zum Beispiel im Winter, bei kalten Temperaturen, erfolgt die Kühlung der Flächen mit deutlich geringerem Stromverbrauch. E-Shelter ist zudem das erste RZ in der Schweiz, das die Norm ISO50001 erfüllt hat.

Internetanbindung

Die Internetanbindung von cloudscale.ch erfolgt über zwei unterschiedliche Trassees (sog. Trasseeredundanz) zu den beiden Carrier-meet-me-Räumen im Gebäude. Diese wiederum werden über zwei separate Hauseinführungen (auf gegenüberliegenden Gebäudeseiten) erschlossen. cloudscale.ch verwendet bewusst zwei verschiedene Carrier mit unterschiedlichen

Hardware-Lieferanten (Init7 mit Brocade/Extreme-Equipment, Liberty Global mit Cisco-Equipment) und ist zusätzlich am SwissIX Internet Exchange präsent. cloudscale.ch betreibt das Autonome System 59414. https://bgp.he.net/AS59414#_asinfo

Welche technischen Massnahmen zum Schutz des Hosts (Host Firewalls, regelmässige Integritätsüberprüfungen, Host-based Intrusion Detection Systems) sind implementiert?

Netzwerk

Physische Separierung von Management- und Kunden-Traffic (Separates, redundantes Netzwerkequipment, Multi-Vendor-Strategie)
Physische Separierung von Internet-Access- und Storage-Access-Traffic (Separate, redundante Netzwerkverbindungen)
Logische Separierung von public und private Kunden-Traffic (Dediziertes, privates VXLAN pro Kunde)
IPtables und ebtables auf jedem Compute-Host:
- Jeder virtueller Server (VM) hat ein festgelegtes IP-/MAC-Adress-Paar und kann nur damit kommunizieren
- Unterbindung von man-in-the-middle Attacken im public Netzwerk
- Unterbindung von Sniffing im public Netzwerk
- Dank dediziertem VXLAN komplette, logische Separierung im private Netzwerk

Controller

Physische Separierung der Control-, Compute- und Storage-Hosts
Logische Separierung der Controller-Dienste in LXC-Containern
Management-Zugriff auf die physische Maschine ist nur aus dem dedizierten Management-Netzwerk möglich (keine Exponierung ins Internet)

Compute

Kernelvirtualisierung mit QEMU/KVM (Vollvirtualisierung, separater QEMU Prozess pro VM)
Memory ist fix alloziert pro Kunde, auch bei ausgeschalteter VM (Kein Memory-Ballooning oder Kernel Same-Page Merging)
Viele 0-Day-Sicherheitslücken können dank AppArmor unter Ubuntu gar nicht ausgenutzt werden
Konsequenter Einsatz von ECC-Memory (z.B. Rowhammer-Attacke dadurch praktisch ausgeschlossen)
Management-Zugriff auf die physische Maschine ist nur aus dem dedizierten Management-Netzwerk möglich (keine Exponierung ins Internet)

Storage

Separates RBD Volume pro Kunde und pro Volume in der VM (Replikationsfaktor 3, verteilt auf 3 verschiedene Racks)
Management-Zugriff auf die physische Maschine ist nur aus dem dedizierten Management-Netzwerk möglich (keine Exponierung ins Internet)

Control Panel

Login-Passwörter werden ausschliesslich gesaltet und gehashed abgelegt
Optionale 2-Factor-Authenifizierung (TOTP)
Anzeige von SSH Host Key Fingerprints pro VM
Konsequenter Einsatz von CSRF-Prevention
Session-Management mit -Übersicht

Wie stellt Cloudscale eine sichere Grund-Konfiguration des Hosts (z. B. Einsatz gehärteter Betriebssysteme, Deaktivierung unnötiger Dienste, etc.) sicher?

Für die Sicherstellung der einheitlichen Konfiguration (Firewall-Rules, Deaktivierung von unnötigen Diensten) verwenden wir Ansible als Config Management Tool. Als Betriebssystem setzen wir auf Ubuntu LTS (Long Term Support), welches speziell für den Servereinsatz geeignet ist. Jeder LTS-Release wird während mindestens 5 Jahren nach Erscheinen supported (Security Updates).

Weitere Informationen

Wenn dies gewünscht wird, können zusätzlich zwei Reports von BDO (ISAE 3000 und Revisionsbericht FINMA) gesendet werden, welche viele Fragen zur Sicherheit abdecken werden.

In Absprache mit Joineer darf der Kunde die Architektur von cloudscale.ch gerne auditieren (lassen). CloudScale verrechnet dafür CHF 225 pro Stunde (exkl. MwSt) und das Audit findet zwingend in den Büroräumlichkeiten von Cloudscale statt.