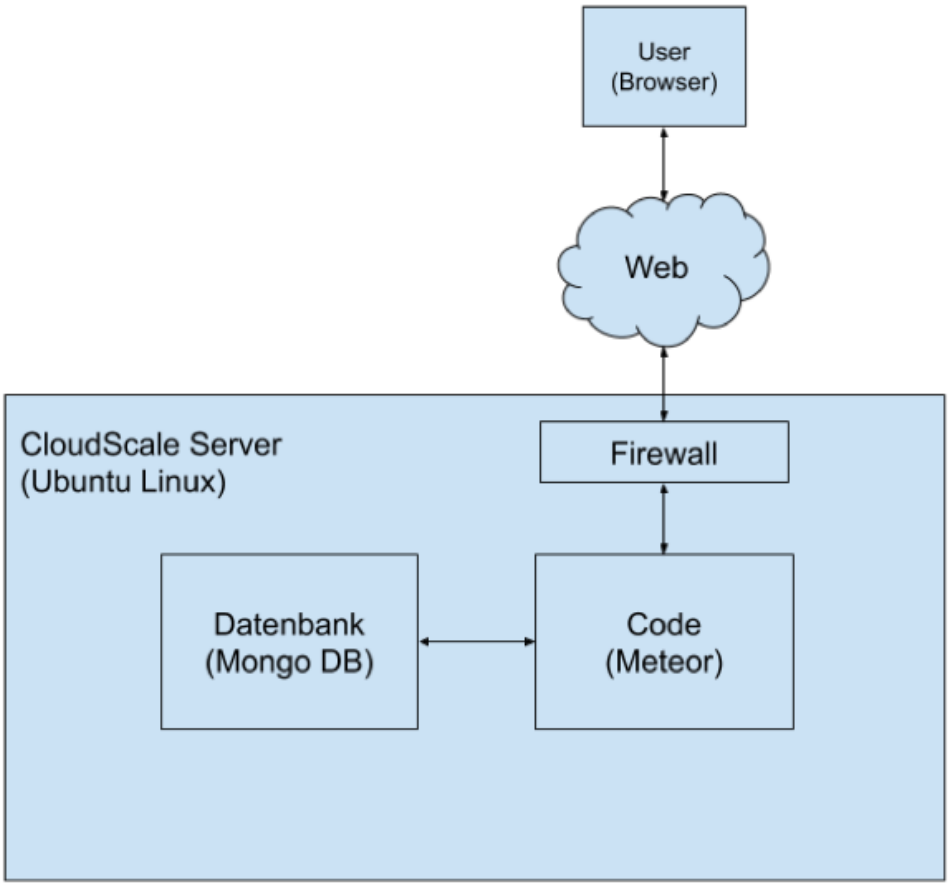
Sommario dell’architettura IT di Joineer AG

Sommario dell’architettura IT di Joineer AG

Schema dell'architettura IT

L'infrastruttura di cloudscale.ch AG è situata presso e-shelter Dataschutz AG a Rümlang, Zurigo in Svizzera.



Il database e il codice di tutti i prodotti Joineer si trovano sul server di Cloudscale.

In seguito, verranno discussi i punti più importanti dell'infrastruttura server di Cloudscale:

Separazione fisica

cloudscale.ch ha una propria cosiddetta gabbia, cioè un'area separata e chiusa all'interno del centro dati, in cui si trovano solo i nostri rack e non è possibile l'accesso a terzi. Il contratto per questa gabbia è stato stipulato per 5 anni (con l'opzione di estendere per altri 5 anni) per essere in grado di garantire il massimo livello di sicurezza fisica a lungo termine.

Alimentazione e ridondanza

In questa gabbia, la corrente proviene da due percorsi diversi e da diverse schede di sub-distribuzione, che a loro volta sono collegate a diverse schede di distribuzione principali, a due diversi binari di alimentazione per rack. In caso di mancanza di corrente, entrambe le distribuzioni principali sono supportate da cluster di UPS separati fino a quando uno dei generatori diesel (ridondanza 2N+1) prende il carico. I due quadri di distribuzione principali sono collegati in un anello a diversi fornitori (EWZ e EKZ). La ridondanza è testata dall'operatore del centro dati a intervalli regolari (i cosiddetti test autarchici).

Tutti i nostri sistemi sono collegati a entrambi i circuiti, in modo da poter far fronte al guasto di un'unità di alimentazione - o di un intero circuito - senza alcun impatto notevole sulle operazioni.

Climatizzazione

L'area del centro dati è priva di tubi che trasportano acqua ed è circondata da un cosiddetto anello di condizionamento (unità di raffreddamento ad aria circolante: ridondanza 2N). L'acqua viene convogliata in un anello in modo che, in caso di guasto, le singole sezioni possano essere interrotte e riparate senza mettere in pericolo la linea di alimentazione delle restanti unità di raffreddamento a ricircolo d'aria. L'edificio ha anche un sistema di free-cooling sul tetto. Questo significa, per esempio, che in inverno, quando le temperature sono fredde, il raffreddamento delle aree avviene con un consumo energetico significativamente inferiore. E-Shelter è anche il primo centro dati in Svizzera a rispettare lo standard ISO50001.

Connessione Internet

La connessione internet di cloudscale.ch verso le due stanze del carrier-meet-me nell'edificio avviene attraverso due percorsi diversi (la cosiddetta ridondanza dei percorsi). Questi, a loro volta, sono collegati tramite due ingressi separati dell'edificio (sui lati opposti dell'edificio).

cloudscale.ch utilizza deliberatamente due diversi carrier con diversi fornitori di hardware (Init7 con apparecchiature Brocade/Extreme, Liberty Global con apparecchiature Cisco) ed è anche

presente su SwissIX Internet Exchange. cloudscale.ch gestisce il sistema autonomo 59414. https://bgp.he.net/AS59414#_asinfo

Quali misure tecniche sono implementate per proteggere l'host (firewall dell'host, controlli regolari dell'integrità, sistemi di rilevamento delle intrusioni basati sull'host)?

Rete

Separazione fisica della gestione e del traffico dei clienti (apparecchiature di rete separate e ridondanti, strategia multi-vendor)
Separazione fisica dell'accesso a Internet e del traffico di accesso allo storage (connessioni di rete separate e ridondanti)
Separazione logica del traffico pubblico e privato dei clienti (VXLAN specifica per cliente).
IPtables e ebtables su ogni host di calcolo:
- Ogni server virtuale (VM) ha una coppia di indirizzi IP/MAC definita e può comunicare solo con essa
- Prevenzione degli attacchi man-in-the-middle nella rete pubblica
- Prevenzione dello sniffing nella rete pubblica
- Completa separazione logica nella rete privata grazie alla VXLAN dedicata

Controller

Separazione fisica degli host di controllo, elaborazione e archiviazione

Separazione logica dei servizi del controller nei contenitori LXC
L'accesso di gestione alla macchina fisica è possibile solo dalla rete di gestione apposita (nessuna esposizione a Internet)

Elaborazione

Virtualizzazione del kernel con QEMU/KVM (virtualizzazione completa, processo QEMU separato per ogni VM)
La memoria è allocata in modo fisso per client, anche quando la VM è spenta (nessun memory ballooning o kernel same-page merging)
Molte vulnerabilità di sicurezza 0-day non possono essere sfruttate nemmeno sotto Ubuntu grazie ad AppArmor
Uso coerente della memoria ECC (es. attacco Rowhammer praticamente impossibile)

L'accesso di gestione alla macchina fisica è possibile solo dalla rete di gestione dedicata (nessuna esposizione a Internet)

Stoccaggio

Volume RBD separato per cliente e per volume nella VM (fattore di replica 3, distribuito su 3 diversi rack). L'accesso di gestione alla macchina fisica è possibile solo dalla rete di gestione apposita (nessuna esposizione a Internet)

Pannello di controllo

Le password di accesso sono esclusivamente commutate e sottoposte ad hash
Autenticazione a 2 fattori opzionale (TOTP)
Visualizzazione delle impronte digitali delle chiavi host SSH per VM
Uso coerente della prevenzione CSRF
Gestione delle sessioni con panoramica

Come fa Cloudscale a garantire una configurazione di base sicura dell'host (ad es. uso di sistemi operativi hardened, disabilitazione di servizi non necessari, ecc.)?

Per assicurare una configurazione coerente (regole del firewall, disabilitazione dei servizi non necessari), usiamo Ansible come strumento di gestione della configurazione. Usiamo Ubuntu LTS (Long Term Support) come sistema operativo, che è particolarmente adatto per l'uso di server. Ogni release LTS è supportata per almeno 5 anni dopo il suo rilascio (aggiornamenti di sicurezza).

Ulteriori informazioni

Se lo si desidera, possono essere inviati due rapporti aggiuntivi da BDO (ISAE 3000 e rapporto di audit FINMA), che coprono molte questioni di sicurezza.

In consultazione con Joineer, il cliente è invitato a verificare l'architettura di cloudscale.ch. CloudScale addebita 225 CHF all'ora (IVA esclusa) per questo e l'audit deve avere luogo presso gli uffici di Cloudscale.