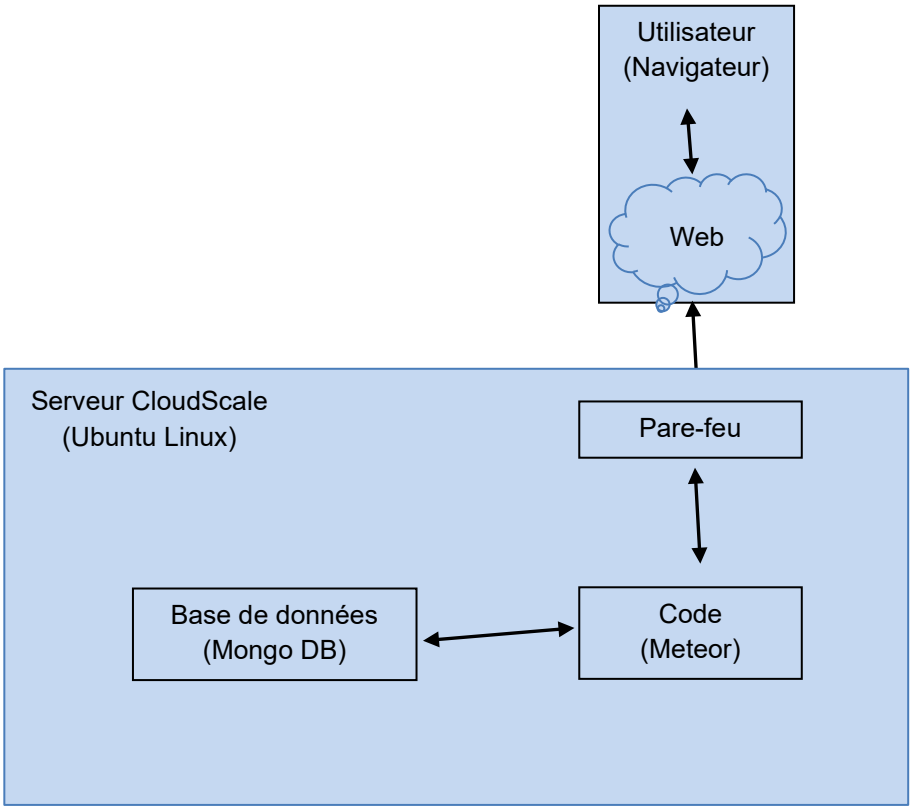
Résumé de l'architecture informatique

Schéma d'architecture informatique

L'infrastructure de cloudscale.ch AG est hébergée chez e-shelter Dataschutz AG à Rümlang, Zurich en Suisse.



La base de données et le code de tous les produits Joineer sont situés sur le serveur de Cloudscale.

Les principaux points de l'infrastructure du serveur Cloudscale sont décrits ci-dessous :

Séparation physique

cloudscale.ch dispose de sa propre cage, c'est-à-dire d'une zone séparée et fermée au sein du centre de données, dans laquelle se trouvent uniquement nos racks et à laquelle aucun tiers n'a accès. Le contrat pour cette cage a été conclu pour 5 ans (avec une option de prolongation de 5 ans supplémentaires) afin de pouvoir garantir le plus haut niveau de sécurité physique à long terme.

Alimentation électrique et redondance

Dans cette cage, l'alimentation est acheminée sur deux routes différentes à partir de différentes sous-distributions, qui sont à leur tour connectées à différentes distributions principales, vers deux rails d'alimentation différents par rack. En cas de panne de courant, les deux tableaux de distribution principaux sont pris en charge par des groupes d'onduleurs distincts jusqu'à ce que l'un des générateurs diesel (redondance 2N+1) reprenne la charge. Les deux tableaux de distribution principaux sont reliés en anneau à des fournisseurs différents (EWZ et EKZ). La redondance est testée par l'exploitant du centre de données à intervalles réguliers (tests dits autarciques). Tous nos systèmes sont connectés aux deux circuits, de telle sorte que nous pouvons faire face à la défaillance d'une unité d'alimentation électrique - ou d'un circuit entier - sans impact notable sur les opérations.

Climatisation

La zone du centre de données est exempte de conduites d'eau et est entourée d'un serpentin de climatisation (unités de refroidissement à air recyclé : redondance 2N). L'eau est acheminée en anneau de sorte qu'en cas de défaut, les sections individuelles peuvent être interrompues et réparées sans mettre en danger la ligne d'alimentation des autres unités de refroidissement à air recyclé. Le bâtiment dispose également d'un système de refroidissement (free-cooling) sur le toit. Cela signifie, par exemple, qu'en hiver, lorsque les températures sont froides, le refroidissement des zones s'effectue avec une consommation d'énergie nettement inférieure. Par ailleurs, E-Shelter est le premier centre de données en Suisse à être conforme à la norme ISO50001.

Connexion internet

La connexion internet de cloudscale.ch s'effectue via deux routes différentes (ce que l'on appelle la redondance des routes) vers les deux salles de réunion des opérateurs dans le bâtiment. Ces derniers sont à leur tour accessibles par deux entrées distinctes du bâtiment (sur les côtés opposés du bâtiment). cloudscale.ch utilise délibérément deux opérateurs différents avec une protection des données différente. cloudscale.ch utilise délibérément deux opérateurs différents

avec des fournisseurs de matériel différents (Init7 avec du matériel Brocade/Extreme, Liberty Global avec du matériel Cisco) et est également présent sur le SwissIX Internet Exchange. cloudscale.ch exploite le système autonome 59414. https://bgp.he.net/AS59414#_asinfo

Quelles mesures techniques sont mises en œuvre pour protéger l'hôte (pare-feu de l'hôte, vérifications régulières de l'intégrité, systèmes de détection des intrusions basés sur l'hôte) ?

Réseau

Séparation physique du trafic de gestion et du trafic client (équipements de réseau séparés et redondants, stratégie multi-fournisseurs).
Séparation physique du trafic d'accès à internet et du trafic d'accès au stockage (connexions réseau distinctes et redondantes).
Séparation logique du trafic client public et privé (VXLAN privé et spécifique au client).

IPtables et ebtables sur chaque ordinateur hébergeant :
- Chaque serveur virtuel (VM) possède une paire d'adresses IP/MAC fixe et ne peut communiquer qu'avec elle.
- Prévention des attaques de type "intermédiaire" dans le réseau public
- Prévention du sniffing (écoute clandestine) dans le réseau public
- Grâce au VXLAN privé et spécifique au client, séparation logique complète dans le réseau privé.

Contrôle

Séparation physique du dispositif de contrôle hôte, de l'ordinateur hébergeant et du dispositif de stockage hôte
Séparation logique des services de contrôle dans les conteneurs LXC.
L'accès de gestion à la machine physique n'est possible qu'à partir du réseau de gestion réservé à cet effet (aucune exposition à internet).

Traitement des données

Virtualisation du noyau avec QEMU/KVM (virtualisation complète, processus QEMU séparé par VM).
La mémoire est allouée de façon permanente par client, même lorsque la VM est éteinte (pas de gonflement de la mémoire ni de fusion de pages identiques dans le noyau).
De nombreuses failles de sécurité de type "0-jour" ne peuvent pas être exploitées sous Ubuntu grâce à AppArmor.

Utilisation cohérente de la mémoire ECC (par exemple, l'attaque Rowhammer est pratiquement impossible).
L'accès de gestion à la machine physique n'est possible qu'à partir du réseau de gestion réservé à cet effet (aucune exposition à internet).

Stockage

Volume RBD distinct par client et par volume dans la VM (facteur de réplication 3, réparti sur 3 racks différents).
L'accès de gestion à la machine physique n'est possible qu'à partir du réseau de gestion réservé à cet effet (aucune exposition à internet).

Panneau de contrôle

Pour le stockage des mots de passe de connexion, uniquement le salage et le hachage sont utilisés.
Authentification à deux facteurs en option (TOTP)
Affichage des empreintes de la clé de l'hôte SSH par VM
Utilisation cohérente de la prévention CSRF
Gestion des sessions avec vue d'ensemble

Comment Cloudscale assure-t-il une configuration de base sécurisée de l'hôte (par exemple, l'utilisation de systèmes d'exploitation renforcés, la désactivation de services inutiles, etc.)

Pour assurer une configuration uniforme (règles de pare-feu, désactivation des services inutiles), nous utilisons Ansible comme outil de gestion de configuration. Nous utilisons Ubuntu LTS (Long Term Support = Support à long terme) comme système d'exploitation, qui est particulièrement adapté à l'utilisation de serveurs. Chaque version LTS est supportée pendant au moins 5 ans après sa sortie (mises à jour de sécurité).

Informations complémentaires

Si vous le souhaitez, nous pouvons en plus vous envoyer deux rapports de BDO (rapport d'audit ISAE 3000 et FINMA), qui couvriront de nombreuses questions de sécurité. En concertation avec Joineer, le client est invité à auditer (ou à faire auditer) l'architecture de cloudscale.ch. CloudScale facture 225 CHF par heure (hors TVA) pour cela et l'audit doit avoir lieu dans les bureaux de Cloudscale.