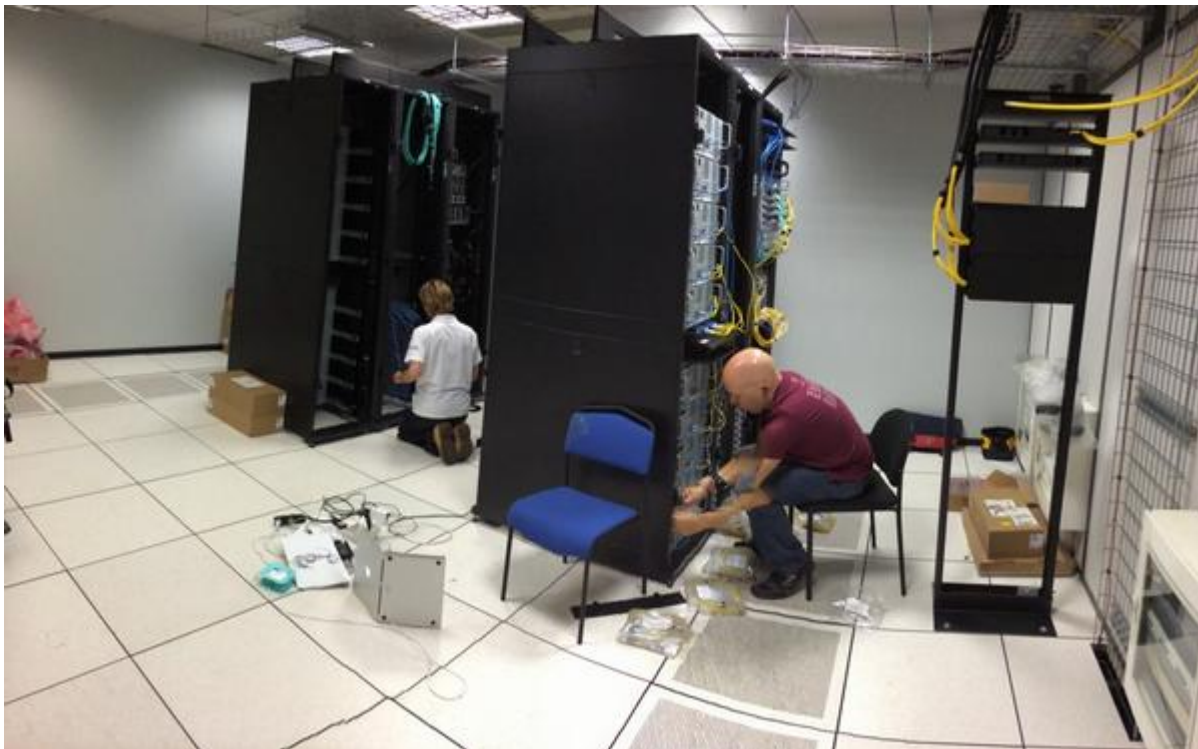


Netflix : une architecture IT taillée pour le succès

Après des mois de discussions et bravés les courroux ministériels ainsi que ceux des opérateurs (sauf Bouygues Telecom qui accueillera le service à son démarrage), le service de VoD Netflix se lance en France. Mais derrière l'aspect commercial, Netflix s'est aussi une architecture IT bien huilée avec des capacités importantes.

Les travaux sur la partie datacenter en France ont commencé en 2014 avec une présence au **sein du centre de calcul de TeleHouse à Paris**, boulevard Voltaire, un des centres névralgiques du trafic en France. **David Tamkin**, le responsable des réseaux chez le diffuseur américain avait publié [une photo sur Twitter](#) (ci-dessous) du début de ce déploiement. La partie réseau a du répondant avec une bande passante prévue à **1 Tbit/s**. Dans ce cadre, Netflix a signé un accord avec France IX, le point d'échange Internet pour une bande passante de **100 Gb/s**, « **la plus forte commande à ce jour** », indiquait fin juillet **Franck Simon**, directeur général de France IX, à l'AFP. Pour Telehouse, cette bande passante totale équivaut « **à un fournisseur d'accès internet avec 5 millions de clients** ». Pour les puristes David Tamkin a même fourni quelques éléments sur les équipements réseaux, à savoir des switches 7508 d'Arista et des routeurs MX480 de Juniper Networks.



Sur la partie infrastructure, la présence de Netflix restera cantonnée à ce point de présence et de transit, car la société fait reposer son offre en matière de serveurs et de stockage sur une architecture complètement Cloud au sein d'AWS (Amazon Web Services). Un reportage réalisé par nos confrères de [Businessweek](#) en mai 2013 montrait que le diffuseur gérait **4 millions d'heures de programme tous les quart d'heure** sur plus de 1000 terminaux différents. Le catalogue maître de Netflix nécessitait **3, 14 Po d'espace de stockage**. A titre de comparaison Facebook gère 1,5 Po de

stockage pour ces 10 milliards de photos. Toujours en matière de stockage, le service de VoD analyse chaque jour les contenus les plus populaires et utilisent du stockage flash pour les mettre plus rapidement à disposition des clients. Les vidéos moins demandées seront conservées sur des disques durs traditionnels moins chers.

Un optimisateur d’AWS et un spécialiste sécu

Cette relation proche avec AWS permet à Netflix de travailler sur des services d’optimisation. Récemment, il a mis à disposition de tous, [sur GitHub](#), un outil spécifique qu’il a développé pour **superviser la sécurité de son infrastructure Cloud**. [Opérationnelle depuis 2011](#) (dans sa première version), cette solution de sécurité, de monitoring et d’analyse, appelée **Security Monkey**, vise à améliorer la connaissance des changements et risques sur un environnement AWS. La solution se décompose en 3 modules : **Watcher** qui détecte et enregistre des changements de configurations dans les environnements AWS S3, IAM et EC2; **Notifier**, un système d’alerte; et **Auditor**, qui rapproche les règles métier des configurations AWS pour isoler des divergences et détecter des risques. S’y ajoute un système de gestion de règles, que les utilisateurs peuvent enrichir. On notera aussi que Security Monkey rejoint **la Simian Army** (l’armée simiesque), une **suite d’outils développés par Netflix** pour tester la fiabilité, la sécurité ou la résilience d’AWS. Ces outils (Chaos Monkey, Latency Monkey, Conformity Monkey, Doctor Monkey, Janitor Monkey...) sont disponibles pour la plupart en Open Source.

Par ailleurs, en dehors de son implication pour améliorer la résilience d’AWS, Netflix s’intéresse aussi aux autres questions de sécurité. Il a ainsi mis à disposition de tous une solution [pour surveiller Internet et détecter des attaques planifiées contre ses infrastructures](#). Notamment les DDoS, les attaques par déni de service susceptibles de mettre en péril sa qualité de service, un critère évidemment central pour un diffuseur de vidéos comme Netflix. Cette solution se compose de trois outils distincts. Le premier, baptisé **Scumblr**, **passé les forums et les médias sociaux au peigne fin** à la recherche de discussions sur des projets de hacking ou d’attaques DDoS. Il s’appuie sur **Workflowable**, outil permettant de créer des workflows flexibles associés à des résultats de recherche. Une sorte de **gare de triage pour l’outil de recherche**. Enfin, Scumblr est associé à **Sketchy**, qui prend automatiquement des captures d’écran ou capture les textes des résultats dénichés par le moteur de recherche.

A lire aussi :

[Netflix met le chaos dans le cloud d’Amazon](#)

[Netflix nettoie AWS en mode open source](#)