

Capture du trafic ACI Cisco

Enjeu

De nombreuses entreprises déploient des solutions ACI Cisco en raison de l'évolutivité, de la haute disponibilité et des capacités d'orchestration offertes par cette architecture réseau. Toutefois, cette solution soulève plusieurs problématiques, à la fois en matière de visibilité et de déploiement des outils de monitoring et de sécurité.

- Les volumes de trafic sont très élevés, ce qui implique un coût très élevé des outils.
- Le trafic est encapsulé en de nombreux points (VxLAN, QinQ), ce qui rend impossible une identification adéquate.
- Pour obtenir une visibilité complète du trafic est-ouest, il est nécessaire d'obtenir une capture consolidée du trafic physique et du trafic virtuel.
- L'architecture doit présenter une évolutivité progressive, pour accompagner le déploiement.
- Enfin, il doit être possible de connecter des outils en tout point, pour une haute disponibilité et un bon équilibrage des systèmes.

Solution

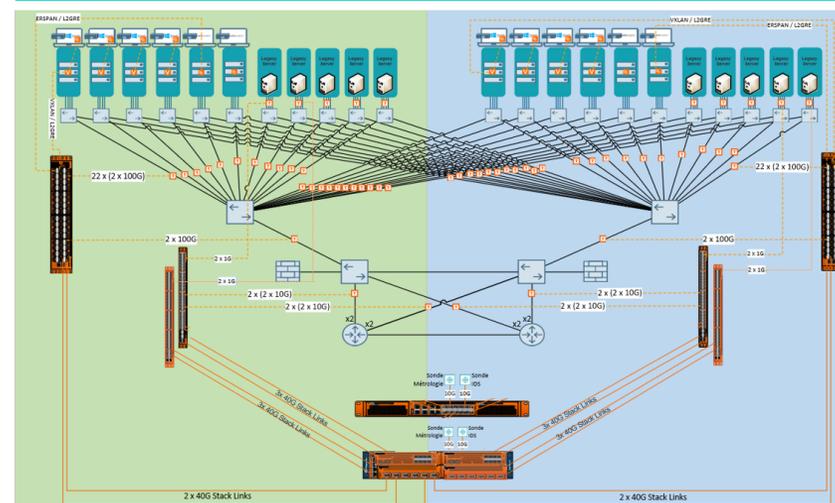
L'architecture Gigamon peut être mise en correspondance avec celle de Cisco dans un schéma Spine&Leaf. Elle peut ainsi opérer un déploiement parallèle au réseau ACI, pour fournir une haute disponibilité et un équilibrage des outils connectés.

La solution de Gigamon s'adapte en déployant différentes options, pour une visibilité TOTALE sur le trafic :

- Des TAP physiques sur les liens du réseau entre les couches du Spine&Leaf, avec la possibilité de retirer les balises VxLan du NFV tout en identifiant chacun des services ou Building Blocks.
- Des TAP virtuels pour les infrastructures informatiques déployées via Cisco APIC.
- Création de cartes et de règles dans la solution Gigamon Packet Broker, pour que chaque outil de sécurité et de monitoring puisse recevoir le trafic approprié.
- Automatisation totale grâce à l'API de Gigamon et à l'intégration avec Ansible.

L'intégralité du système se comporte comme un ensemble de ressources partagées, piloté par un seul outil de gestion, le Fabric Manager. Ce dernier peut être programmé par l'API pour orchestrer des déploiements automatiques.

Architecture



Licences

- TAP
- Agrégateurs NPB V-Series
- Fabric Manager
- Tunneling
- Header Stripping
- Déduplication

LIEN