asprom

Radar GigaOm pour Service Mesh (Interconnecter l'entreprise)

Un maillage de services (Service Mesh) est une couche d'infrastructure dédiée qui permet de gérer la communication entre les microservices d'une application. Il agit essentiellement comme un intermédiaire, fournissant des fonctionnalités telles que la gestion du trafic, la sécurité et l'observabilité.

Voici un aperçu de son fonctionnement :

- **Architecture des microservices** : Les applications modernes sont souvent créées à l'aide de microservices, qui sont de petits services indépendants qui travaillent ensemble pour atteindre un objectif plus vaste. Cela peut rendre la communication entre les services complexe.
- **Proxy de side-car** : Un maillage de services utilise un proxy léger appelé proxy sidecar. Ce proxy est déployé à côté de chaque microservice et intercepte l'ensemble de son trafic réseau.
- **Contrôle centralisé** : Le maillage de services est contrôlé par une entité centrale qui configure les proxys side-car et dicte la façon dont le trafic circule entre les services.

Les avantages de l'utilisation d'un maillage de services sont les suivants :

- **Gestion simplifiée de la communication** : En déchargeant la gestion de la communication sur le maillage de services, les développeurs n'ont pas à s'en soucier dans leur code, ce qui rend le développement plus rapide et plus facile.
- **Sécurité améliorée** : Le maillage de services peut appliquer des stratégies de sécurité telles que l'authentification et l'autorisation, garantissant ainsi que seuls les services autorisés peuvent communiquer entre eux.
- **Observabilité améliorée** : Le maillage de services fournit des informations sur la façon dont les microservices communiquent, ce qui facilite le diagnostic et le débogage des problèmes.

Si vous travaillez avec des architectures de microservices, un maillage de services peut être un outil précieux pour simplifier le développement, améliorer la sécurité et obtenir une meilleure visibilité sur votre application.

1. Résumé

Jouant un rôle essentiel dans le développement **cloud natif,** un maillage de services permet des communications rapides, fiables et sécurisées entre les microservices. Contrairement à d'autres systèmes de gestion des communications intra-service, un maillage de services est une couche d'infrastructure dédiée entièrement intégrée au sein de l'application. Mis en œuvre soit parallèlement à la charge de travail en tant que proxy

side-car, soit intégré directement dans le service ou la plate-forme elle-même, un maillage de services élimine la complexité, la fragmentation et les vulnérabilités de sécurité liées au codage répété des communications de service à service en externalisant la gestion des demandes vers un fournisseur externe. application du processus.
Comme il s'agit d'une technologie émergente en constante évolution, le choix d'un maillage de services nécessite que les décideurs évaluent soigneusement le paysage, en tenant compte de la complexité, de la latence et de la consommation de ressources supplémentaires impliquées. Avec divers fournisseurs open source et commerciaux ciblant un large éventail d'environnements d'application et d'options de déploiement, ce **rapport GigaOm Radar** fournit un aperçu des maillages de services offerts par les projets open source et les enjeux de table basés sur le paysage des fournisseurs, les critères clés et l'évaluation. métrique. La figure 1 répertorie les maillages de services inclus dans ce rapport et leurs options d'acquisition.

SERVICE MESH PROJECTS AND VENDORS GIGAOM

SERVICE MESH	HOST/ VENDOR	OPEN SOURCE (FREE)	COMMERCIAL (PAID)	ISTIO-BASED
Anthos Service Mesh	Google	-	X	X
AWS App Mesh	Amazon	-	X	-
Cilium Service Mesh	CNCF	X	X	-
F5 Aspen Mesh	F5	-	X	X
Gloo Mesh	Solo.io	-	X	X
Greymatter	greymatter.io	-	X	-
HashiCorp Consul	HashiCorp	X	X	-
Istio	CNCF	X	-	X
Kong Mesh	Kong	-	X	-
Kuma	CNCF	X	-	-
Linkerd	CNCF	X	-	-
Network Service Mesh	CNCF	X	-	-
OpenShift Service Mesh	Red Hat	X	X	X
Tanzu Service Mesh	VMware	-	X	X
Traefik Mesh	Traefik Labs	X	X	-

Source: GigaOm 2023

Remarque : Assurant la gouvernance des projets cloud natifs open source et indépendants des fournisseurs, la Cloud Native Computing Foundation (CNCF) héberge plusieurs projets open source pilotés par la communauté avec différents niveaux de maturité : bac à sable (stade précoce), incubation (stable), ou diplômé (largement déployé dans les environnements de production).

Avec différentes options de maillage de services et un paysage en évolution rapide, le choix du meilleur maillage de services pour votre organisation dépend de vos cas d'utilisation, de la pile logicielle existante, des choix architecturaux et des capacités internes. De plus, vos ressources et compétences internes influenceront votre décision quant à savoir si vous adoptez un maillage de services léger et convivial pour les développeurs ou une solution complète nécessitant des services professionnels.
Ce rapport GigaOm Radar met en évidence les principaux projets et fournisseurs de services maillés et fournit les informations dont les décideurs informatiques ont besoin pour sélectionner la meilleure solution pour leur entreprise et leurs cas d'utilisation. Le rapport GigaOm correspondant « Critères clés pour l'évaluation des solutions de maillage de services » décrit plus en détail les capacités et les mesures utilisées pour évaluer les fournisseurs sur ce marché.
C'est la troisième année que nous évaluons l'espace du maillage de services dans le contexte de nos rapports Critères clés et Radar. Toutes les solutions incluses dans ce rapport Radar répondent aux enjeux suivants : des capacités largement adoptées et bien mises en œuvre dans le secteur :

- Couche d'infrastructure dédiée
- Authentification de service à service
- Configuration du plan de contrôle
- Télémétrie du plan de contrôle

2. Catégories de marché et types de déploiement

Pour mieux comprendre le marché et le positionnement du fournisseur (**Tableau 1**), nous évaluons dans quelle mesure un maillage de services open source ou fournisseur prend en charge différents segments de marché cibles et modèles de déploiement.

Pour ce rapport, nous reconnaissons les segments de marché suivants :

- **Fournisseur de services cloud (CSP) :** fournisseurs fournissant des services à la demande et payants à l'utilisation aux clients sur Internet, notamment une infrastructure en tant que service (IaaS), une plate-forme en tant que service (PaaS) et un logiciel en tant que service (SaaS). .
- **Fournisseur de services réseau (NSP) :** les fournisseurs de services vendant des services réseau, tels que l'accès au réseau et la bande passante, fournissent des points d'entrée à l'infrastructure de base ou aux points d'accès réseau (NAP). Dans ce rapport, les NSP incluent les opérateurs de données,

les FAI, les opérateurs de télécommunications et les fournisseurs de services sans fil.
- **Fournisseur de services gérés (MSP) :** fournisseurs de services fournissant des services gérés d'applications, de communication, d'infrastructure informatique, de réseau et de sécurité, ainsi qu'un support aux entreprises dans les locaux du client ou via MSP (hébergement) ou des centres de données tiers (colocation).
- **Grande entreprise :** entreprises de 1 000 employés ou plus dotées d'équipes informatiques dédiées chargées de la planification, de la création, du déploiement et de la gestion de leurs applications, de leur infrastructure informatique, de leurs réseaux et de leur sécurité dans un centre de données sur site ou dans une installation de colocation.
- **Petites et moyennes entreprises (PME) :** petites entreprises (moins de 100 employés) et entreprises de taille moyenne (100 à 1 000 employés) avec des budgets limités et des ressources internes limitées pour la planification, la création, le déploiement et la gestion de leurs applications. Infrastructure informatique, réseaux et sécurité dans un centre de données sur site ou dans une installation de colocation.

De plus, nous reconnaissons les modèles de déploiement suivants :

- **Cluster unique ou multiple** : les maillages de services peuvent être configurés soit comme un seul cluster, soit comme un seul maillage comprenant plusieurs clusters. Un déploiement en cluster unique peut offrir de la simplicité, mais il lui manque des fonctionnalités telles que l'isolation des pannes, le basculement et l'isolation des projets qui sont disponibles dans un déploiement multicluster.
- **Réseau unique ou multiple** : les instances de charge de travail directement connectées sans utiliser de passerelle résident dans un seul réseau, permettant une configuration uniforme des consommateurs de services à travers le maillage. Une approche multiréseau permet à un maillage de services de couvrir diverses topologies ou sous-réseaux de réseau, offrant ainsi conformité, isolation, haute disponibilité et évolutivité.
- **Plan de contrôle unique ou multiple** : le plan de contrôle configure toutes les communications entre les instances de charge de travail au sein du maillage. Le déploiement de plusieurs plans de contrôle sur des clusters, des régions ou des zones permet une isolation de la configuration, un contrôle précis des déploiements de configuration et une isolation du niveau de service. De plus, si un plan de contrôle devient indisponible, l'impact de la panne est limité aux charges de travail gérées par ce plan de contrôle.
- **Maillage unique ou multiple** : bien qu'un seul maillage puisse s'étendre sur un ou plusieurs clusters ou réseaux, les noms de services sont uniques au sein du maillage. Étant donné que les espaces de noms sont utilisés pour la location, un maillage fédéré est requis pour découvrir les services et

communiquer au-delà des limites du maillage. De plus, chaque maillage révèle des services qui peuvent être consommés par d'autres services, fournissant ainsi des limites au secteur d'activité et une isolation entre les charges de travail de test et de production.

	SEGMENT DE MARCHÉ					MODÈLE DE DÉPLOIEMENT			
	Fournisseur de services de chiffrement	PSN	MSP	Grande entreprise	PME	Cluster unique ou multiple	Réseau unique ou multiple	Plan de contrôle unique ou multiple	Maillage simple ou multiple
Amazone	–	–	–	+++	++	+++	–	–	–
Cil (CNCF)	+	++	++	+++	+	+++	++	+	++
F5	++	+++	+++	+++	++	++	++	++	++
Google	–	–	–	++	+++	++	–	++	++
matière grise.io	++	++	++	+++	++	+++	+++	+++	+++
HashiCorp	++	+	+	+++	+++	++	++	++	++
Istio (CNCF)	++	+	+	+++	++	++	++	++	+
Kong	–	–	–	+++	++	+++	+++	+++	+++
Kuma (CNCF)	–	–	–	+++	++	++	+++	+++	+++
Linkerd (CNCF)	–	–	–	+++	++	++	++	++	++
Maillage de services réseau (CNCF)	++	++	++	+++	++	+++	+++	+++	+++
chapeau rouge	–	–	–	+++	++	++	++	++	++
Solo.io	+++	+++	+++	+++	++	++	++	++	++
Laboratoires Traefik	+	+	+	++	+++	+++	++	+	+
VMware	++	++	+++	+++	+	++	++	++	++

- *** Exceptionnel : concentration et exécution exceptionnelles
- ** Capable : Bon mais avec marge d'amélioration
- * Limité : manque d'exécution et de cas d'utilisation
- - Sans objet ou absent

3. Comparaison des critères clés

S'appuyant sur les conclusions du rapport GigaOm, « Critères clés pour l'évaluation des solutions de maillage de services », les tableaux 2, 3, 4 et 5 résument les performances de chaque projet ou fournisseur inclus dans cette recherche dans les domaines que nous considérons différenciants et critiques dans ce domaine. secteur.

Des critères clés différencient les solutions en fonction de leurs fonctionnalités et capacités, décrivant les principaux critères à prendre en compte lors de l'évaluation d'un maillage de services, notamment la résilience intégrée, la sécurité convergée et l'automatisation AIOps.
Les mesures d'évaluation fournissent un aperçu des exigences non fonctionnelles pertinentes pour les décisions d'achat, reflétant des aspects fondamentaux, notamment la configurabilité, l'interopérabilité et l'observabilité.
Les technologies émergentes identifient les technologies les plus convaincantes et potentiellement les plus impactantes émergentes dans un secteur de produit ou de service au cours des 12 à 18 prochains mois.

Les capacités spécifiques du maillage de services différencient un maillage de services d'un autre en fonction des fonctionnalités spécifiques requises pour fournir des communications de service à service rapides, résilientes et sécurisées.
L'objectif est de donner au lecteur un aperçu des capacités techniques des solutions disponibles, de définir le périmètre du paysage du marché et d'évaluer l'impact potentiel sur l'entreprise.

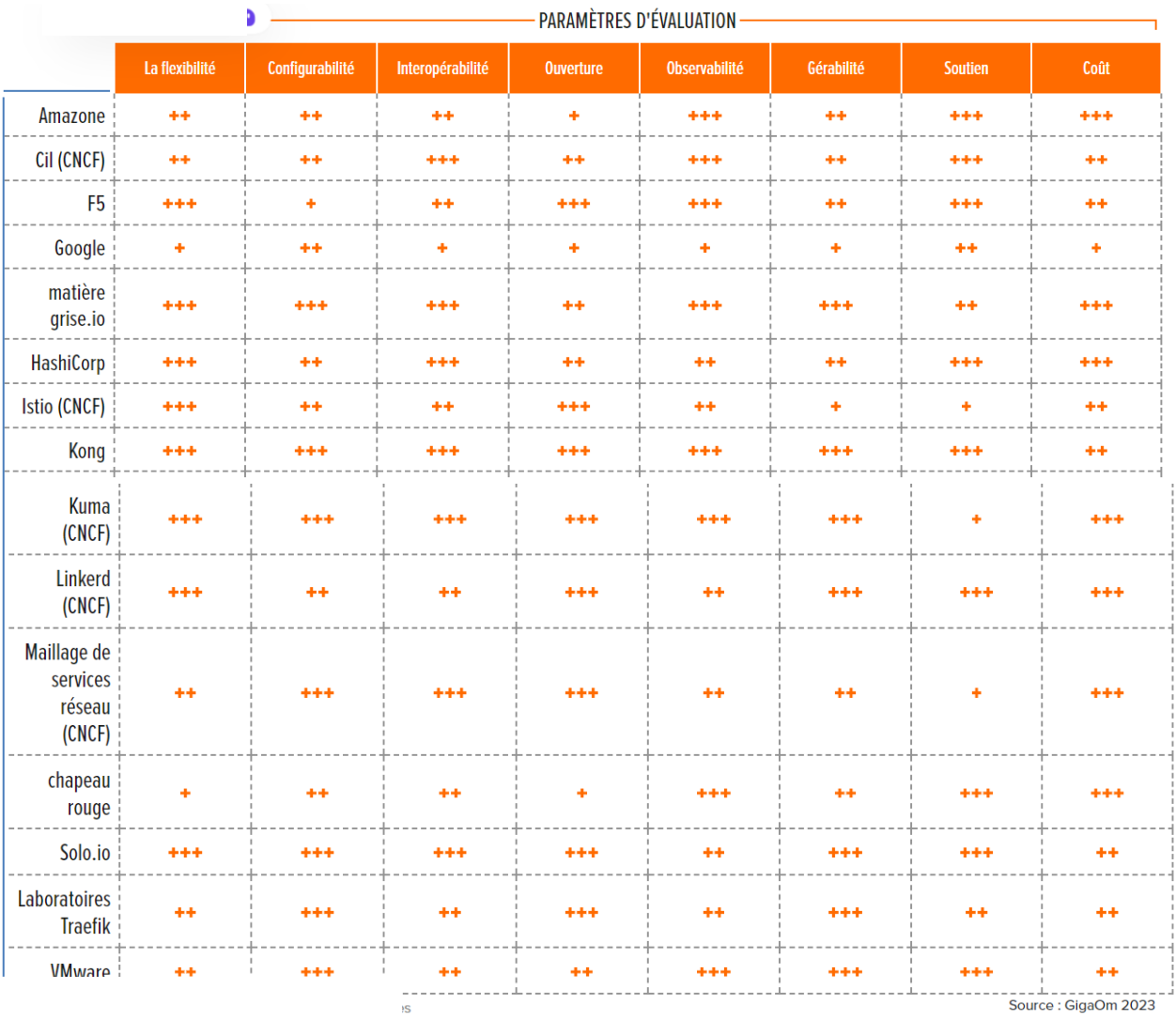
Tableau 2. Comparaison des critères clés

	CRITÈRES CLÉS						
	Prise en charge de la plateforme	Implémentation du side-car	La consommation de ressources	Faible latence	Résilience intégrée	Sécurité convergée	Automatisation AIOps
Amazone	+	++	++	+++	++	++	+
Cil (CNCF)	++	+	++	+++	+	++	–
F5	++	++	+	+	++	+++	+
Google	+	++	++	++	+++	++	–
matière grise.io	+++	+++	++	++	++	+++	+++
HashiCorp	+++	++	+++	+++	++	+++	–
Istio (CNCF)	+++	++	++	++	++	++	+
Kong	+++	++	++	++	+++	+++	++
Kuma (CNCF)	+++	++	+++	++	++	++	–
Linkerd (CNCF)	+	+++	+++	+++	+++	+++	–
Maillage de services réseau (CNCF)	++	++	+++	+++	++	++	–
chapeau rouge	+	++	++	++	++	++	–
Solo.io	+++	+++	++	++	+++	+++	++
Laboratoires Traefik	++	–	+++	++	++	+	+
VMware	+++	+++	++	++	+++	+++	+++

+++ Exceptionnel : concentration et exécution exceptionnelles
++ Capable : Bon mais avec marge d'amélioration
+ Limité : manque d'exécution et de cas d'utilisation
– Sans objet ou absent

Source : GigaOm 2023

Tableau 3. Comparaison des mesures d'évaluation



	PARAMÈTRES D'ÉVALUATION							
	La flexibilité	Configurabilité	Interopérabilité	Ouverture	Observabilité	Gérabilité	Soutien	Coût
Amazone	++	++	++	+	+++	++	+++	+++
Cil (CNCF)	++	++	+++	++	+++	++	+++	++
F5	+++	+	++	+++	+++	++	+++	++
Google	+	++	+	+	+	+	++	+
matière grise.io	+++	+++	+++	++	+++	+++	++	+++
HashiCorp	+++	++	+++	++	++	++	+++	+++
Istio (CNCF)	+++	++	++	+++	++	+	+	++
Kong	+++	+++	+++	+++	+++	+++	+++	++
Kuma (CNCF)	+++	+++	+++	+++	+++	+++	+	+++
Linkerd (CNCF)	+++	++	++	+++	++	+++	+++	+++
Maillage de services réseau (CNCF)	++	+++	+++	+++	++	++	+	+++
chapeau rouge	+	++	++	+	+++	++	+++	+++
Solo.io	+++	+++	+++	+++	++	+++	+++	++
Laboratoires Traefik	++	+++	++	+++	++	+++	++	++
VMware	++	+++	++	++	+++	+++	+++	++

Source : GigaOm 2023

– Sans objet ou absent

+++ *Exceptionnel : concentration et exécution exceptionnelles*

++ *Capable : Bon mais avec marge d'amélioration*

= *Limité : manque d'exécution et de cas d'utilisation*

_ *Sans objet ou absent*

Tableau 4. Comparaison des technologies émergentes

	TECHNOLOGIE ÉMERGENTE				
	Implémentation sans side-car	Assemblage Web	OPA	Réseaux 5G et Edge	SMaaS
Amazone	–	–	–	++	++
Cil (CNCF)	+++	+	++	+++	–
F5	–	+++	++	+++	–
Google	–	–	–	++	–
matière grise.io	++	++	+++	++	+++
HashiCorp	–	–	–	++	+++
Istio (CNCF)	+++	+++	+	–	–
Kong	+	+	+++	++	++
Kuma (CNCF)	+	+	–	++	–
Linkerd (CNCF)	–	+	++	+++	+++
Maillage de services réseau (CNCF)	–	–	++	++	–
chapeau rouge	–	++	–	–	–
Solo.io	+++	+++	+++	+	–
Laboratoires Traefik	+++	–	–	–	–
VMware	+	+++	+++	++	+++

+++ Exceptionnel : concentration et exécution exceptionnelles
++ Capable : Bon mais avec marge d'amélioration
+ Limité : manque d'exécution et de cas d'utilisation
- Sans objet ou absent

Tableau 5. Comparaison des capacités spécifiques du maillage de services

	CAPACITÉS SPÉCIFIQUES DU MAILLAGE DE SERVICES						
	Découverte de services	Routage avancé	Traçage distribué	Chiffrement	Disjoncteur	Injection de défauts	L'équilibrage de charge
Amazone	+	++	++	++	++	+	+++
Cil (CNCF)	++	++	++	++	++	++	++
F5	++	++	++	++	+++	++	++
Google	++	++	+	++	++	++	+
matière grise.io	+++	+++	+++	+++	++	++	+++
HashiCorp	+++	++	++	+++	++	–	+++
Istio (CNCF)	++	++	++	++	+++	+++	++
Kong	+++	+++	++	+++	++	++	+++
Kuma (CNCF)	+++	+++	++	++	++	++	+++
Linkerd (CNCF)	++	++	++	+++	++	+	+++
Maillage de services réseau (CNCF)	++	++	–	++	–	–	+
chapeau rouge	++	++	++	++	++	++	++
Solo.io	+++	+++	+++	+++	++	+++	+++
Laboratoires Traefik	++	++	++	+	++	–	++
VMware	+++	+++	+++	+++	+++	++	+++

+++ Exceptionnel : concentration et exécution exceptionnelles
++ Capable : Bon mais avec marge d'amélioration
+ Limité : manque d'exécution et de cas d'utilisation
- Sans objet ou absent

En combinant les informations fournies dans les tableaux ci-dessus, le lecteur peut développer une compréhension claire des solutions techniques disponibles sur le marché.

4. Radar GigaOm

Ce rapport synthétise l'analyse des critères clés et leur impact sur les mesures d'évaluation pour éclairer le graphique GigaOm Radar de la figure 1. Le graphique résultant est une perspective prospective sur tous les fournisseurs de ce rapport en fonction des capacités techniques et des ensembles de fonctionnalités de leurs produits. .

Le radar GigaOm trace les solutions des fournisseurs sur une série d'anneaux concentriques, ceux situés plus près du centre étant jugés avoir une valeur globale plus élevée. Le graphique caractérise chaque fournisseur sur deux axes (équilibre entre maturité et innovation et jeu de fonctionnalités et jeu de

plateforme), tout en fournissant une flèche qui projette l'évolution de chaque solution au cours des 12 à 18 mois à venir.

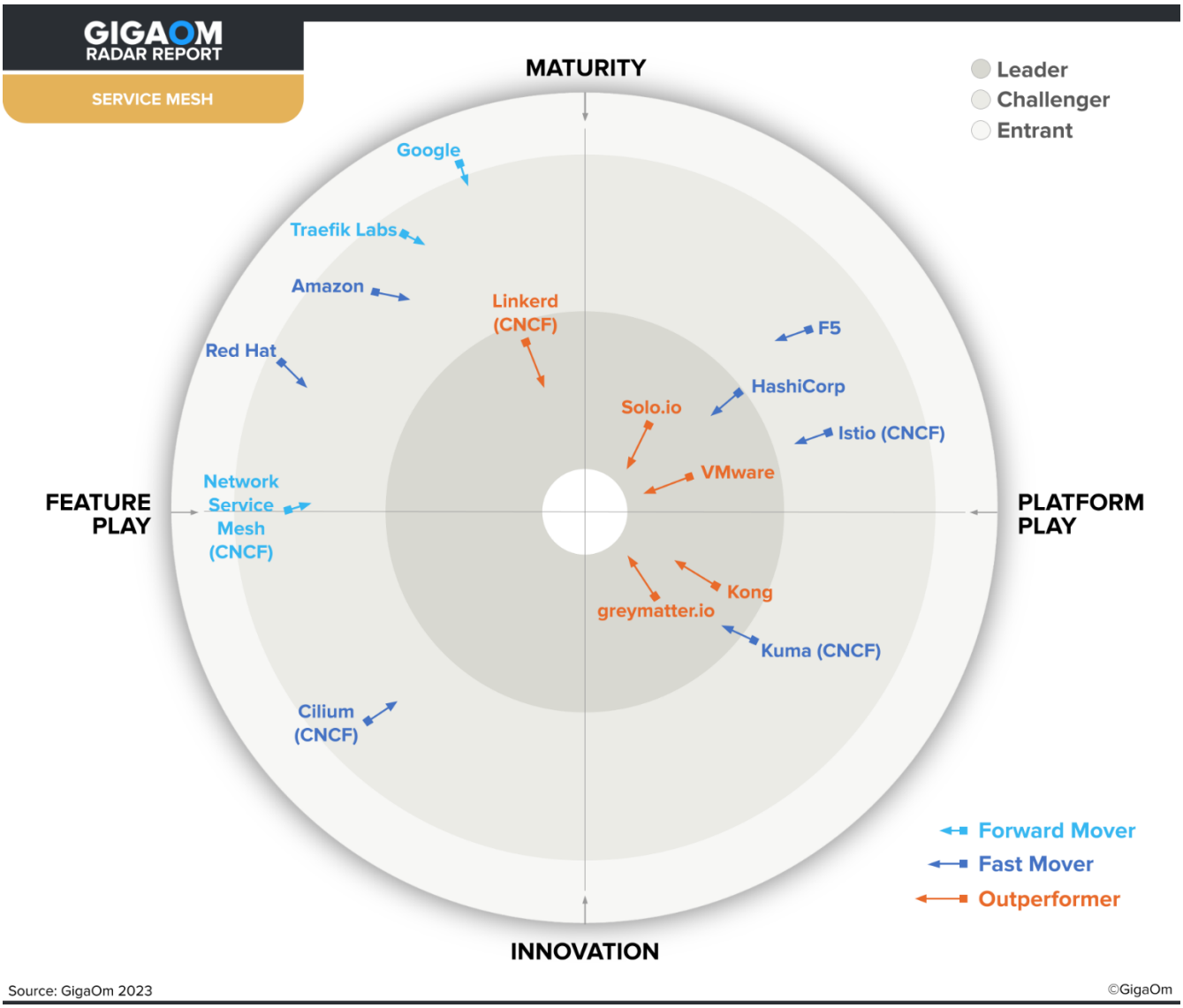


Figure 2. Radar GigaOm pour Service Mesh

Il convient de noter que la Maturité n'exclut pas l'Innovation. Au lieu de cela, il identifie la solution comme ayant fait ses preuves dans un environnement de production par rapport à une solution plus récente en cours d'innovation pour être acceptée et adoptée par les clients. De plus, la longueur de la flèche (Forward Mover, Fast Mover ou Outperformer) est basée sur l'exécution par rapport à la feuille de route et à la vision (selon les commentaires du projet ou du fournisseur dans le rapport de l'année dernière et par rapport aux améliorations apportées dans l'industrie en général).

De plus, le positionnement dans les quadrants Platform-Play indique que le maillage de services inclut les fonctionnalités généralement attendues d'un maillage de services et peut être déployé sur un large éventail de plates-formes

même si le projet ou le fournisseur se concentre sur un ensemble limité de cas d'utilisation. En revanche, certains maillages de services sont positionnés dans les quadrants Feature-Play pour les raisons suivantes :

- Le maillage de services prend en charge une gamme limitée de plates-formes (AWS App Mesh, Anthos Service Mesh, Linkerd, OpenShift Service Mesh et Traefik Service Mesh).
- Le maillage de services possède un ensemble limité de fonctionnalités (Network Service Mesh).
- Le maillage de services inclut les fonctionnalités généralement attendues d'un maillage de services mais avec une architecture nouvelle et évolutive (Cilium Service Mesh).

Comme le montre la figure 2 , Gloo Mesh, Greymatter, Kong Mesh, Linkerd et Tanzu Service Mesh sont reconnus comme surperformants. Gloo Mesh et Tanzu Service Mesh continuent d'être les principaux maillages de services basés sur Istio. Gloo Mesh intègre l'architecture sans side-car d'Istio Ambient Mesh, les meilleures pratiques intégrées en matière d'extensibilité et de sécurité, ainsi qu'une gestion simplifiée et centralisée du cycle de vie d'Istio et d'Envoy, tandis que Tanzu Service Mesh évolue rapidement en tant que composant central de la stratégie de microservices cloud natifs de VMware. Repoussant les limites grâce à une innovation continue, Greymatter offre une visibilité exceptionnelle sur les couches 3, 4 et 7, une intelligence inégalée, une prise en charge intégrée des cas d'utilisation émergents et une optimisation automatisée des performances. Plate-forme full-stack hautement portable et indépendante du cloud, fonctionnant partout, Kong Mesh offre une facilité d'utilisation et des capacités d'automatisation intégrées comme alternative aux solutions open source plus complexes, difficiles à déployer et à gérer. Enfin, Linkerd continue d’être rapidement adopté car il est ultraléger, ultrarapide et simple à déployer sur le plan opérationnel.

Un maillage de services à surveiller est Cilium Service Mesh. En concurrence avec Istio Ambient Mesh, le projet Cilium a été le premier maillage de services à offrir la flexibilité d'exécuter un maillage de services soit dans un modèle side-car exploitant le plan de contrôle de l'API Gateway, soit dans un modèle sans side-car avec un choix de plans de contrôle pour une efficacité accrue. Alors que le jury n'a pas encore déterminé les avantages et les risques liés à l'intégration de l'eBPF dans un maillage de services, plusieurs projets et fournisseurs le font ou l'ont inclus dans leurs feuilles de route.

Depuis la publication du GigaOm Radar for Service Mesh 2022, Istio est passé de Leader à Challenger en raison du fait que les maillages de services basés sur Istio dépassent le maillage de services communautaire en termes d'innovation. De plus, Open Service Mesh et NGINX Service Mesh de CNCF ont tous deux été supprimés. NGINX Service Mesh a été financé et n'est plus pris en charge par F5, tandis que le projet Open Service Mesh a été archivé et ses responsables réaffectés au projet Istio.

L'INTÉRIEUR DU RADAR GIGAOM

Le radar GigaOm évalue l'exécution, la feuille de route et la capacité à innover de chaque fournisseur pour tracer des solutions selon deux axes, chacun étant défini comme des paires opposées. Sur l'axe Y, la maturité reconnaît la stabilité de la solution, la force de l'écosystème et une position conservatrice, tandis que l'innovation met en avant l'innovation technique et une approche plus agressive. Sur l'axe X, Feature Play implique une focalisation étroite sur des fonctionnalités de niche ou de pointe, tandis que Platform Play affiche une approche plus large de la plate-forme et un engagement envers un ensemble complet de fonctionnalités.

Plus une solution est proche du centre, meilleures sont son exécution et sa valeur, les plus performants occupant le cercle intérieur des leaders. Le cercle le plus central est presque toujours vide, réservé aux marchés très matures et consolidés qui manquent d'espace pour davantage d'innovation.

Le radar GigaOm propose une évaluation prospective, traçant la position actuelle et projetée de chaque solution sur une fenêtre de 12 à 18 mois. Les flèches indiquent les voyages en fonction de la stratégie et du rythme de l'innovation, les fournisseurs étant désignés comme Forward Movers, Fast Movers ou Outperformers en fonction de leur taux de progression.

Notez que le Radar exclut la part de marché des fournisseurs comme mesure. L'accent est mis sur une analyse prospective qui met l'accent sur la valeur de l'innovation et de la différenciation par rapport à la position actuelle sur le marc

5. Informations sur les fournisseurs

5 – 1 -Amazon : AWS App Mesh- https://aws.amazon.com/fr/app-mesh/

Lancé lors d'AWS re:Invent 2018, **AWS App Mesh** est un service entièrement géré offrant les avantages d'un maillage de services aux clients Amazon Web Services (AWS) utilisant des services de calcul et de conteneur. Fournissant une mise en réseau au niveau des applications pour exécuter des applications à grande échelle, AWS App Mesh peut être utilisé avec des conteneurs de microservices gérés par Amazon Elastic Container Services (ECS), Amazon Elastic Container Service for Kubernetes (EKS), AWS Fargate, Kubernetes sur EC2 et les services en cours d'exécution. sur Amazon Elastic Compute Cloud (EC2). App Mesh s'intègre également à AWS Outposts pour les applications exécutées sur site et utilise une version personnalisée du proxy open source Envoy, ce qui le rend compatible avec un large éventail de partenaires AWS et d'outils open source.

Prenant en charge à la fois les conteneurs et les machines virtuelles, AWS App Mesh crée une couche d'abstraction basée sur des nœuds, des routeurs, des routes et des services virtualisés. Le plan de contrôle App Mesh est conçu pour prendre en charge les services de calcul AWS, et le proxy Envoy est personnalisé pour prendre en charge le

plan de contrôle. Les utilisateurs incluent le proxy dans la définition de tâche ou de pod de chaque microservice et configurent le conteneur d'application du service pour communiquer directement avec le proxy. Agent for Envoy surveille les proxys Envoy et aide à les maintenir en bonne santé, rendant les applications plus résilientes aux pannes. De plus, App Mesh fournit une API (accessible via AWS PrivateLink pour éviter d'exposer les données à l'Internet public) pour configurer les itinéraires de trafic et d'autres contrôles entre les microservices activés par le maillage, permettant aux utilisateurs d'acheminer le trafic en fonction du chemin ou des poids vers des services spécifiques. versions de service.

Les clients peuvent tirer parti d'App Mesh en ajoutant l'image proxy Envoy à la définition de tâche (Amazon ECS et AWS Fargate) à l'aide du contrôleur AWS App Mesh open source, soit en muté le contrôleur d'admission du webhook (EKS), soit en exécutant le proxy Envoy en tant que conteneur ou processus sur une instance EC2 et rediriger le trafic réseau via le proxy. Lorsque chaque service démarre, le proxy se connecte automatiquement au plan de contrôle et est configuré par App Mesh. Une fois configuré, App Mesh gère la configuration d'Envoy pour fournir des fonctionnalités de maillage de services, équilibrant automatiquement la charge du trafic de tous les clients du maillage et exportant des métriques, des journaux et des traces vers les points de terminaison spécifiés dans la configuration d'amorçage d'Envoy.

App Mesh utilise la sécurité mutuelle de la couche de transport (mTLS) pour l'authentification de la couche de transport de service à service, permettant aux clients d'étendre le périmètre de sécurité en fournissant des certificats à partir d'une autorité de certification privée AWS Certificate Manager ou d'une autorité de certification gérée par le client, appliquant ainsi l'authentification automatique pour les applications clientes. connexion aux services. De plus, la télémétrie générée par AWS App Mesh, telle que les taux d'erreur et les connexions par seconde, peut être exportée vers Amazon CloudWatch et AWS X-Ray ou diffusée vers des services de surveillance tiers, notamment Flagger, Grafana, Jaeger, Prometheus et Splunk, ainsi que des solutions de traçage ouvert comme LightStep et Zipkin.

Points forts :

Service géré enfichable Kubernetes (K8s) hautement disponible, AWS App Mesh est entièrement intégré au paysage AWS, ce qui permet aux clients de surveiller et de gérer facilement les communications pour les microservices sans avoir besoin d'installer ou de gérer une infrastructure supplémentaire au niveau des applications. Le vaste écosystème AWS, la base installée et la position sur le marché stimuleront l'adoption et le développement d'AWS App Mesh. AWS App Mesh est gratuit pour les clients AWS.

Défis :

En tant que service géré, AWS App Mesh est limité à la prise en charge des applications exécutées sur AWS et ne peut pas être migré vers d'autres environnements. App Mesh est également propriétaire, utilise une version personnalisée d'Envoy, ne prend pas en

charge l'interface SMI (Service Mesh Interface) et peut être plus complexe à configurer que les autres maillages de services natifs K8.

5 – 2 - Cilium Service Mesh- https://cilium.io/use-cases/service-mesh/

Lancé en juillet 2022, **Cilium Service Mesh** étend les capacités de mise en réseau, de sécurité et d'observabilité de Cilium au niveau du protocole d'application et est le premier maillage de services à offrir la flexibilité d'exécuter soit un modèle side-car exploitant le plan de contrôle Istio, soit un modèle sans side-car avec un choix. des avions de contrôle. Créé par Isovalent et offert à la CNCF en tant que projet d'incubation en octobre 2021, Cilium est un plug-in open source offrant mise en réseau, observabilité et sécurité pour les serveurs nus, les clusters K8 et autres plates-formes d'orchestration de conteneurs et VM. En tant qu'interface réseau de conteneurs (CNI), Cilium utilise eBPF pour insérer dynamiquement une puissante logique de contrôle dans le noyau Linux, permettant ainsi d'appliquer et de mettre à jour les politiques de sécurité de Cilium sans nécessiter de modification du code de l'application ou de la configuration du conteneur.

Cilium Service Mesh permet aux entreprises de choisir entre un modèle side-car basé sur Envoy et un modèle sans side-car basé sur Envoy plus eBPF. Alors qu'un maillage de services typique basé sur un proxy dissocie de nombreuses fonctions (y compris la découverte de services, la sécurité de la couche de transport (TLS), les tentatives et l'équilibrage de charge) du code de l'application et les place dans un side-car, Cilium Service Mesh va encore plus loin dans le découplage. Combinant les politiques de couche 7, l'observabilité et les capacités de gestion du trafic du proxy Envoy avec les capacités de la technologie eBPF au niveau du noyau pour le trafic réseau de couche 4 et inférieure, Cilium permet d'exécuter ces mêmes fonctions par nœud plutôt que par pod.

Framework for Everyone (SPIFFE) comme options de plan de contrôle. De plus, toutes les fonctionnalités du plan de données Envoy sont disponibles via une définition de ressource personnalisée (CRD Le modèle sans side-car prend en charge l'API Gateway et le Secure Production Identity) Kubernetes. Le contrôleur Ingress intégré, qui exploite Envoy et eBPF, peut être appliqué au trafic entrant dans un cluster K8s et entre les clusters pour un équilibrage de charge et une gestion du trafic riches en fonction de la couche 7, y compris le routage basé sur le chemin, la terminaison TLS et le partage d'une charge unique. -équilibreur IP pour plusieurs services. Les versions futures prendront en charge des plans de contrôle de maillage de services supplémentaires, à commencer par SMI et l'initiative GAMMA de l'API K8s Gateway pour les cas d'utilisation du maillage de services.

L’approche sans side-car promet une complexité réduite, une latence plus faible et une consommation de ressources plus efficace grâce aux performances et aux conflits de démarrage et d’arrêt du side-car. Étant donné que de nombreux paquets n'ont pas besoin d'être acheminés via le proxy pour accéder aux informations de couche 7, les

performances sont augmentées en les transmettant directement via eBPF vers l'interface réseau, réduisant ainsi la latence et accélérant le démarrage du pod. Un analyseur HTTP de couche 7 hautes performances avec prise en charge d'OpenTelemetry fournit un traçage à une fraction du coût d'une solution basée sur un proxy.

Fonctionnalité destinée aux utilisateurs expérimentés, Cilium Service Mesh comprend CiliumEnvoyConfig (CEC), une abstraction de bas niveau pour programmer les proxys Envoy directement avec une nouvelle définition de ressource personnalisée (CRD) K8 pour les cas d'utilisation avancés de la couche 7 afin de rendre l'ensemble complet des fonctionnalités Envoy disponible pour utilisateurs. Simplifiant l'intégration de plans de contrôle de maillage de services supplémentaires, CEC permet au contrôleur d'entrée Cilium de spécifier les auditeurs Envoy et d'autres ressources, permettant ainsi de rediriger de manière transparente le trafic destiné à des services K8 spécifiques vers ces auditeurs Envoy. De plus, Cilium ClusterMesh permet aux services exécutés sur plusieurs clusters d'être regroupés en un seul service global, offrant ainsi la possibilité de voir les événements de sécurité sur plusieurs clusters.

Points forts :

Cilium Service Mesh permet aux utilisateurs d'exécuter un maillage de services avec ou sans side-car en fonction de la disponibilité, de la gestion des ressources et des considérations de sécurité. Un choix de plans de contrôle offre un équilibre entre simplicité (Kubernetes Ingress et Gateway API) et puissance (Envoy et Istio). Isovalent offre un support aux entreprises et diverses améliorations, notamment une observabilité avancée du réseau et un proxy DNS hautement disponible. Cilium Service Mesh est disponible en téléchargement gratuit depuis GitHub ou en version entreprise avec le support d'Isovalent.

Défis :

bien que le déploiement d'un maillage de services et le déchargement du travail sur eBPF lorsque cela est logique soient compréhensibles, le découplage du proxy de l'application dans le modèle sans side-car introduit une couche supplémentaire de complexité et d'imprévisibilité opérationnelle et de sécurité. Les avantages en termes de performances de l'option sans side-car plus simple, à faible latence et efficace de Cilium peuvent être compensés lorsque les utilisateurs

5 – 3 - F5 : Aspen Mesh F5 - https://www.f5.com/fr_fr/products/aspen-mesh

Start-up incubée au sein de F5 (anciennement F5 Networks), **F5 Aspen Mesh** a été lancée en décembre 2017 en tant que distribution de maillage de services basée sur Istio, entièrement prise en charge, prête pour la production et renforcée en termes de sécurité, conçue pour gérer les infrastructures K8 matures et complexes. Prenant en charge les fournisseurs de services mobiles nécessitant une entrée et une sortie IPv4/IPv6 double pile pour le contrôle, les données et la signalisation, F5 Aspen Mesh intègre une sécurité multicloud zéro confiance, l'application des politiques de conformité, l'observabilité au niveau du protocole et l'optimisation des applications basée sur SRE. Tirant parti de

l'infrastructure mondiale de F5, F5 Aspen Mesh offre une assistance 24h/24 et 7j/7 par concierge pour les environnements de production, avec des options de suivi du soleil et des ingénieurs d'assistance à la demande parlant natif.

F5 Aspen Mesh réduit la complexité d'Istio grâce à la gestion du cycle de vie, aux versions de support à long terme (LTS) et à des services supplémentaires, ajoutant des fonctionnalités avancées à la distribution open source. Ceux-ci incluent une gestion mTLS simplifiée, un contrôle d'accès précis basé sur les rôles (RBAC), Istio Vet (pour découvrir les applications utilisateur incompatibles et les configurations de composants Istio dans un cluster K8s) et l'authentification unique (SSO). De plus, des cadres politiques de reconnaissance d'informations axés sur les objectifs et basés sur l'IA/ML permettent aux utilisateurs de spécifier, mesurer et appliquer des objectifs commerciaux.

Un tableau de bord cloud natif offre une expérience utilisateur intuitive, simplifiant les opérations quotidiennes et permettant d'exécuter en toute sécurité des milliers de conteneurs avec un déploiement, une mise à l'échelle, une application des politiques de sécurité et une résolution des problèmes standardisés. Prenant en charge une infrastructure distribuée et hautement évolutive basée sur les données, le cadre d'observabilité de F5 Aspen Mesh, Rapid Resolve, utilise des analyses de données robustes et un ML conçu pour fournir des informations exploitables en temps réel et réduire le temps moyen de résolution (MTTR) avec des fonctionnalités avancées. capacités de dépannage et de création de rapports sur l'environnement. Le Packet Inspector de F5 Aspen Mesh fournit également une observabilité au niveau du protocole avec des données de télémétrie fournies dans des formats standardisés pour le secteur des télécommunications.

Une solution commune avec F5, BIG-IP Next Service Proxy for Kubernetes (BIG-IP Next SPK) apporte des fonctionnalités réseau critiques à un environnement K8, répondant aux exigences d'un réseau de fournisseur de services. BIG-IP Next SPK prend en charge le contrôle d'entrée/sortie pour la signalisation 4G et 5G tout en rationalisant les transitions vers la 5G autonome (5G-SA) et non autonome (5G-NSA) tout en tirant parti des investissements dans la 4G. La solution offre l'authentification, le cryptage, l'observabilité, la sécurité, la gestion des politiques et la capture de paquets du trafic est/ouest au sein de chaque cluster K8 de base 5G. Dans le même temps, un proxy sécurisé et un pare-feu par service protègent le trafic nord/sud entrant et sortant des services 5G conteneurisés. De plus, F5 Aspen Mesh a ajouté des fonctionnalités Istio personnalisées, notamment la cryptographie à courbe elliptique et la gestion avancée des certificats.

L'un des principaux contributeurs aux communautés Istio et Envoy, F5 a été le premier fournisseur non fondateur à publier et gérer une version d'Istio. La société a abandonné le financement de son maillage de services propriétaire d'origine, NGINX Service Mesh, au profit de F5 Aspen Mesh basé sur Istio et Envoy open source. La tarification

est basée sur un modèle d'abonnement OpEx par nœud avec des services payants en option.

Points forts :

Leader sur le marché des fournisseurs de services, F5 Aspen Mesh est la seule solution basée sur Istio déployable dans le cadre d'un cœur 5G-SA ou 5G-NSA prenant en charge la migration des fonctions de réseau virtualisé (VNF) 4G vers les fonctions de réseau conteneurisées (CNF) de l'architecture basée sur les services (SBA) de la 5G. BIG-IP Next SPK apporte des fonctionnalités critiques de niveau opérateur à un environnement Kubernetes, permettant aux fournisseurs de services réseau de créer un pont entre leurs réseaux 4G existants et un réseau central 5G cloud natif.

Défis :

avec plusieurs fournisseurs fournissant un support de niveau entreprise pour Istio, F5 Aspen Mesh doit trouver des moyens de se différencier auprès des entreprises clientes. Dans le même temps, cependant, F5 Aspen Mesh est souvent accessible via des fournisseurs de services fournissant une infrastructure de services maillée aux entreprises et des services dérivés de services maillé aux consommateurs sur des plates-formes mobiles. De plus, alors que BIG-IP Next SPK constitue un différenciateur crucial pour les NSP, F5 Aspen Mesh devrait simplifier l'expérience Istio pour les entreprises matures dotées d'infrastructures complexes et développer des informations exploitables et assistées par machine pour aider à relever les défis des clients.

5 – 4 - Google : Anthos Service Mesh-

https://cloud.google.com/anthos/service-mesh?hl=fr

Annoncé en septembre 2019, **Anthos Service Mesh (ASM**) est une distribution Istio limitée testée par Anthos permettant aux clients de déployer un maillage de services entièrement pris en charge sur site à l'aide de Google Kubernetes Engine (GKE) sur site, sur Google Cloud ou en tant que solution hybride. solution. En appliquant l'authentification via mTLS, ASM exploite les API Istio et les composants principaux pour offrir agilité, observabilité et sécurité aux services déployés sur Anthos GKE ou sur des déploiements cloud hybrides et sur site avec des services basés sur des conteneurs et des VM.

En remplaçant Istio sur GKE, Google propose Anthos Service Mesh sous la forme d'un plan de contrôle sur site, dans le cluster, d'un maillage de services entièrement géré ou d'un maillage de services hybride couvrant à la fois les déploiements Google Cloud et sur site. Répondant aux besoins des clients VMware existants disposant d'environnements de gestion et d'exploitation familiers, la version sur site utilise GKE On-Prem exécuté sur VMware vSphere sur le matériel du client.

Comprenant Traffic Director, Managed CA et les outils d'exploitation de Google Cloud, la version entièrement gérée d'ASM fournit un plan de données géré en option et un plan de contrôle géré par Google fonctionnant en dehors des clusters Anthos GKE,

réduisant ainsi les frais de gestion tout en garantissant la disponibilité la plus élevée possible. En minimisant la maintenance manuelle des utilisateurs, Google gère la disponibilité, l'évolutivité et la sécurité du plan de contrôle, y compris les correctifs et les mises à niveau logicielles. L'utilisation du plan de contrôle géré par Google simplifie la configuration du maillage multicluster et réduit les privilèges Kubernetes Engine nécessaires pour installer Anthos Service Mesh.

Le plan de données géré par Google est activé en ajoutant simplement une annotation aux espaces de noms, qui installe un contrôleur intégré au cluster pour gérer les proxys side-car. Le plan de données est déployé comme un ensemble de proxys distribués qui assurent la médiation de tout le trafic réseau entrant et sortant entre les services individuels. Les proxys sont configurés à l'aide d'un plan de contrôle centralisé et d'une API ouverte, permettant l'automatisation des tâches réseau quotidiennes, notamment la mise en œuvre de la répartition ou du pilotage du trafic entre les services et l'activation de l'authentification et du chiffrement de service à service.

Même si l'ASM entièrement géré réduit le besoin de ressources internes et augmente la disponibilité et la stabilité, il présente de nombreuses limitations, notamment l'absence de prise en charge des filtres Envoy personnalisés, d'IPv6, de la surveillance cloud proxy TCP interne, des side-cars whitebox ou des environnements multiréseaux. Les environnements externes à Google Cloud, notamment Anthos sur site, Anthos sur d'autres cloud publics, Amazon EKS, Microsoft AKS et d'autres clusters Kubernetes (K8s), ne sont pas pris en charge. Le traçage est limité à Google Cloud Trace, le traçage Jaeger et Zipkin étant disponible uniquement en tant qu'option gérée par le client. De plus, tous les clusters GKE doivent être contenus dans une seule région avec une limite de 1 000 services et 5 000 charges de travail par cluster.

Points forts :

Anthos Service Mesh entièrement géré offre des fonctionnalités de maillage de services de base aux clients Google Anthos existants. Tirant parti de GKE On-Prem, la version sur site s'adresse principalement aux clients VMware existants à la recherche d'environnements de gestion et d'exploitation familiers. Anthos Service Mesh est inclus avec les abonnements Anthos et une tarification basée sur le cluster et le client est disponible pour les déploiements autonomes.

Défis :

reliant les utilisateurs à l'écosystème Google, Anthos Service Mesh est une version allégée d'Istio avec de nombreuses fonctionnalités supprimées, notamment la prise en charge d'Istio CA et d'Istio Operator. De plus, certains éléments et fonctionnalités de l'interface utilisateur de la console Google Cloud ne sont disponibles que pour les abonnés Anthos. Les utilisateurs potentiels doivent évaluer soigneusement les limites d'ASM avant de lancer un PoC, en particulier compte tenu de l'incertitude entourant l'avenir d'Anthos compte tenu de son adoption limitée.

5 – 5 - graymatter.io - http://graymatter.io /

Développée en interne et publiée en février 2019 par graymatter.io, Greymatter est une plate-forme de mise en réseau d'applications éprouvée en entreprise offrant une sécurité zéro confiance, une visibilité des couches 3, 4 et 7, une intelligence d'affaires et une optimisation automatisée des performances. Relevant de nombreux défis introduits par une architecture basée sur les services (SBA), Greymatter est construit sur des principes cloud natifs et des technologies open source, permettant une observabilité granulaire basée sur le maillage de services, des heuristiques et des informations analytiques, ainsi que l'automatisation pour optimiser le débit du trafic à travers environnements sur site, multicloud ou hybrides.

Comblant le fossé entre les applications logicielles anciennes et modernes, la plate-forme comprend un plan de contrôle développé en interne pour les SBA et un plan de données side-car Envoy-proxy avec des filtres étendus pour l'acheminement du trafic interne est/ouest. Une passerelle API contrôle les flux de trafic nord/sud. La plate-forme Greymatter fournit une intégration déclarative de la couche réseau d'applications conviviale pour les développeurs, basée sur des modèles, avec des pipelines de livraison CI/CD couvrant tous les environnements sur site et multicloud. En plus de fournir une architecture maillée de cybersécurité prête à l'emploi, la plate-forme s'intègre à Open Policy Agent (OPA) pour un contrôle d'accès sans confiance et basé sur des politiques à chaque point du maillage et est suffisamment flexible et ouverte pour interopérer avec d’autres maillages de services.

Conçu pour traiter la télémétrie du maillage de services basée sur un proxy comme une source de business intelligence, Greymatter exploite l'IA et le ML pour analyser les données, y compris les informations réseau des couches 3, 4 et 7, pour une optimisation automatisée des performances et un contrôle des ressources. Alimentées par des auto-encodeurs neuronaux récurrents, les capacités de détection d'anomalies de la plateforme capturent les infimes incohérences opérationnelles, prédisent les problèmes potentiels et alertent les utilisateurs des incohérences via une interface utilisateur contextuelle intuitive pour des mesures correctives.

La plateforme Greymatter prend en charge une variété de cas d'utilisation émergents, notamment la cybersécurité et le maillage de données. Un maillage de cybersécurité est une couche fondamentale permettant à des services de sécurité discrets de fonctionner ensemble de manière transparente, créant ainsi un environnement de sécurité dynamique basé sur une architecture zéro confiance. Permettant la propriété des données fédérées et la gouvernance distribuée, un maillage de données facilite le partage rapide et sécurisé, sans confiance, des objets et des capacités de données sensibles, y compris la provenance des données basée sur des politiques et le suivi de la lignée. La plateforme travaille avec des tiers dans les deux cas pour permettre une prise de décision

intelligente en matière de réseau pour une cybersécurité et une protection des données améliorées.

Greymatter est conçu pour être indépendant de la plate-forme et parler couramment de nombreuses langues. La plateforme regroupe les investissements informatiques existants dans un réseau omniprésent de couches 3, 4 et 7, connectant en toute sécurité les couches existantes des opérations et du système de support commercial (OSS/BSS) aux technologies cloud natives. Capable de fonctionner sur n'importe quelle plateforme d'orchestration de conteneurs publique, privée, hybride, multicloud ou de conteneurs, la plateforme est livrée avec une prise en charge intégrée de K8, AWS EKS, AKS, OpenShift OCP, OKD, Konvoy et bare metal. Il est également indépendant des conteneurs, prenant en charge Docker, CoreOS, K8s, OpenShift, Rancher et d'autres conteneurs, ou aucun conteneur. La plateforme prend également en charge une intégration transparente avec les cadres d'observabilité d'entreprise, notamment DataDog, Elasticsearch, Grafana, Jaeger, LightStep, Splunk et Zipkin.

Fournissant un moteur complet de conformité d'audit et une autorisation d'identité SPIFFE/SPIRE prête à l'emploi, Greymatter fournit des rapports de conformité d'audit de service sans instrumentation spéciale. Les audits en temps réel aux couches 3, 4 et 7 fournissent une source unique de vérité pour chaque utilisateur et chaque action sur le maillage tout au long de la durée de vie de chaque objet. Prenant en charge des clients qualifiés dans des cloud hébergés privés et publics, graymatter.io propose à la fois des services SMaaS et entièrement gérés. Le prix de l'abonnement est basé sur l'environnement.

Points forts :

En plus de fournir une plate-forme multi-environnements robuste, prête pour l'entreprise, indépendante des conteneurs, le sous-système de santé de l'IA basé sur l'heuristique de Greymatter offre un aperçu du bien-être général du réseau avec la capacité de déterminer les causes profondes. analyse et découvrir de nouvelles connaissances opérationnelles sur la façon dont le réseau est utilisé. De plus, les fonctionnalités d'infrastructure en tant que code (IaC) GitOps prêtes à l'emploi permettent une application transparente et cohérente des correctifs de service et des mises à niveau de versions tout en réduisant les risques opérationnels tels que la dérive de la configuration des charges de travail.

Défis :

Greymatter.io est dans une phase de croissance alors qu'elle passe d'une petite entreprise amorcée principalement axée sur les clients du gouvernement américain et du ministère de la Défense à une société de capital-risque soutenant des clients mondiaux couvrant une variété de secteurs industriels. De plus, l'entreprise doit étendre la prise en charge d'autres modules de mise en réseau d'applications pour inclure l'orchestration des IAM des fournisseurs de cloud, des passerelles API des fournisseurs de cloud et des contrôleurs d'entrée des fournisseurs de cloud.

5 – 6 -HashiCorp : Consul HashiCorp - https://local.hashicorp.com/fr

Développé en interne à partir de zéro et publié sous forme de service mesh en octobre 2018, **HashiCorp Consul** offre des capacités de découverte cohérentes et une communication sécurisée de service à service dans n'importe quel environnement. En tant que responsable principal, HashiCorp propose une version open source de Consul et une version entreprise avec des fonctionnalités et un support supplémentaires. HCP Consul est un maillage de services entièrement géré en tant que service fonctionnant sur la plateforme cloud HashiCorp (HCP), offrant des déploiements par bouton-poussoir et en libre-service.

HashiCorp Consul fournit un plan de contrôle complet avec des fonctionnalités de découverte de services, de configuration, d'équilibrage de charge dynamique et de segmentation, permettant à chaque fonctionnalité d'être utilisée indépendamment selon les besoins. Comblant l'écart entre les applications et la mise en réseau, Consul propose une approche étape par étape, permettant aux organisations de déployer la découverte de services et le registre de services avant de mettre en œuvre la mise en œuvre du maillage de services. Il offre également l'automatisation de l'infrastructure réseau pour les environnements IP dynamiques. La plate-forme fonctionne immédiatement avec un simple proxy de couche 4 intégré et prend en charge les intégrations de proxy tiers, notamment Envoy. Construite sur l'API Kubernetes Gateway, la passerelle API Consul détermine la manière dont les clients interagissent avec les applications de maillage de services Consul. Contrairement à de nombreux autres maillages de services, Consul peut fonctionner sur du métal nu ou dans un environnement K8 pur, des K8 et des VM hybrides, ou un environnement uniquement VM sans nécessiter de K8.

Proposé sous forme de solution autogérée ou gérée, offrant une flexibilité aux entreprises de toutes tailles, HashiCorp Consul offre une découverte et une connectivité sécurisée pour toute application exécutée sur n'importe quelle infrastructure ou environnement d'exécution. Consul applique l'authentification mutuelle entre les services à l'aide de la distribution ACL, mTLS et CA, fournit des fonctionnalités de multilocation et prend en charge des règles de gestion granulaires du trafic basées sur l'identité du service et les attributs de demande. De plus, Consul s'intègre à HashiCorp Vault, ce qui inclut l'utilisation de l'autorité de certification de Vault pour générer, stocker et faire pivoter automatiquement les certificats TLS pour le contrôle HashiCorp Consul et le plan de données.

HashiCorp Consul offre également des capacités de livraison progressives (prenant en charge les déploiements Canary, la gestion du trafic des couches 4 et 7 et l'observabilité avancée) pour les conteneurs, les machines virtuelles et les environnements nus. Bien qu'il ne s'agisse pas d'une fonctionnalité de maillage de services typique, Consul peut également automatiser les tâches réseau de couche 3, notamment le pare-feu

dynamique, l'équilibrage de charge automatisé et la visibilité des points de terminaison. HashiCorp Consul s'intègre à Terraform pour automatiser les tâches de mise en réseau via un démon appelé Consul-Terraform-Sync (CTS). À mesure que les services évoluent ou que de nouveaux services deviennent disponibles sur le réseau, CTS mettra automatiquement à jour les équilibreurs de charge réseau et les pare-feu, permettant ainsi la découverte et l'utilisation transparentes de nouveaux services.

HashiCorp Consul fournit une vue cohérente de tous les services sur le réseau, y compris les charges de travail non maillées et quels que soient les différents langages et cadres de programmation, pour les services en temps réel tels que la surveillance de l'état de santé et de la localisation. Consul capture les données au niveau du service et les présente aux utilisateurs via une interface utilisateur intégrée ou via des intégrations avec des solutions de traçage d'applications tierces, notamment Jaeger, OpenTelemetry et Zipkin.

Solution extensible et multiplateforme avec des options d'approvisionnement flexibles, HashiCorp Consul prend en charge les déploiements sur site (virtualisés et nus) et dans le cloud, ainsi que plusieurs environnements d'exécution, notamment Amazon ECS, AWS Lambda, HashiCorp Nomad, les distributions K8 et les machines virtuelles. Il offre également des fonctionnalités et des intégrations natives pour les proxys (notamment Envoy, HAProxy et NGINX), les solutions d'entrée (notamment Ambassador et Nginx) et les solutions de surveillance des performances des applications (APM) telles que AppDynamics, Datadog, Dynatrace, Grafana, Prometheus et Splunk. .

Points forts :

HashiCorp Consul est un maillage de services simple et flexible offrant une prise en charge multicluster et des intégrations avec des charges de travail externes hors maillage de services. Contrairement à de nombreux autres maillages de services, Consul peut fonctionner dans un environnement uniquement VM sans nécessiter de K8. HashiCorp Consul est étroitement intégré au portefeuille de HashiCorp, et l'offre SMaaS, HCP Consul, constitue une option attrayante pour les clients de HashiCorp à la recherche de déploiements par bouton-poussoir et en libre-service. HashiCorp Consul est disponible sous forme de SaaS téléchargeable gratuitement à l'utilisation ou via une tarification basée sur la consommation.

Défis :

Avec seulement une petite communauté open source prenant en charge les utilisateurs non-HashiCorp, la principale valeur de HashiCorp Consul est destinée aux utilisateurs HashiCorp existants souhaitant intégrer des K8 dans leur pile HashiCorp. L'écosystème de Consul est limité par rapport à ses concurrents, manquant de prise en charge des intégrations K8 telles que Flagger. HashiCorp développe actuellement des capacités d'observabilité prêtes à l'emploi et simplifie son modèle actuel de fédération des centres de données HashiCorp Consul afin d'éliminer la complexité du client.

5 – 7 -Istio (Projet CNCF)- https://istio.io/

Lancé en mai 2017**, Istio** a été cofondé par **Google, IBM, Lyft** et d'autres contributeurs clés. Cependant, suite aux inquiétudes exprimées par IBM, Oracle et les communautés open-source et cloud-native sur la gouvernance du projet et la décision de Google de faire don de la marque à l'Open Usage Commons (OUC), Istio a été accepté par la CNCF comme projet en incubation. en septembre 2022. Cette décision remplace le contrôle de Google sur les marques et les licences par une entité neutre et la possibilité d'une adoption plus large. La transition unit Istio avec Envoy et K8 sous un même toit et une gouvernance commune.

Istio, l'un des maillages de services les plus matures et les plus complexes disponibles, offre un riche ensemble de fonctionnalités basées sur le proxy Envoy, notamment la découverte dynamique de services, l'authentification de service à service, l'équilibrage de charge, la surveillance, la création de politiques et le routage du trafic. Conçu pour l'extensibilité, Istio offre un plan de contrôle robuste et unifié basé sur K8 pour gérer les K8 (dans les cloud publics ou sur site), les VM et les plans de données nus, prenant en charge un large éventail de besoins de déploiement.

Le projet Istio propose également Istio Ambient Mesh, une architecture en couches sans side-car offrant une interopérabilité transparente avec le plan de données centré sur le side-car Istio. Bien qu'il ne soit pas encore prêt pour la production, Istio Ambient Mesh permet aux utilisateurs de mélanger et d'associer des fonctionnalités side-car et sans side-car en fonction des besoins spécifiques de chaque application. Un proxy zTunnel léger par nœud gère les fonctionnalités de couche 4, telles que l'observabilité de couche 4, le chiffrement mTLS au niveau du pod et les politiques de niveau de service, tandis qu'un proxy Envoy de point de cheminement facultatif par compte de service fournit une politique de niveau application de couche 7, l'observabilité et la gestion du trafic.

Istio dispose de puissantes capacités prêtes à l'emploi d'authentification, d'autorisation et de chiffrement basées sur l'identité, avec des communications de service sécurisées par défaut pour une application cohérente des politiques. Istio offre également un contrôle précis du comportement du trafic en prenant en charge les tests A/B, les déploiements Canary et les déploiements par étapes avec une répartition du trafic basée sur un pourcentage. Il fournit également des fonctionnalités de récupération après panne prêtes à l'emploi avec des politiques et une gestion de routage avancées, notamment des disjoncteurs, des basculements, des injections de pannes, des contrôles d'état, des tentatives et des déploiements par étapes. De plus, son API de configuration et sa couche de politique prennent en charge les contrôles d'accès, de quota et de taux, tandis que les journaux, métriques et traces détaillés offrent une observabilité approfondie dans l'ensemble du cluster avec des tableaux de bord Grafana et Prometheus intégrés et préconfigurés pour l'observabilité.

Cependant, à mesure que de nouvelles fonctionnalités et fonctionnalités sont ajoutées, Istio est devenu notoirement difficile à installer, à configurer et à gérer. Istio résout cette complexité en abandonnant son architecture de microservices au profit d'une approche monolithique, fusionnant plusieurs fonctions auparavant distinctes pour simplifier le maillage de services et minimiser les compromis. Tout en conservant son approche microservices avec des frontières strictes entre le code et ce qui étaient auparavant des services indépendants, les fonctions d'Istio sont présentées à l'administrateur du cluster comme un processus unique. Il convient toutefois de noter qu'Istio ne dispose pas de tableau de bord intégré ; une solution tierce, Kiali, a été conçue comme un module complémentaire pour gérer, visualiser, valider et dépanner Istio.

Bien que cette approche puisse être bonne d'un point de vue technique, le cycle de publication trimestriel d'Istio peut avoir un impact sur la stabilité opérationnelle. De plus, la complexité d'Istio a donné naissance à un écosystème croissant avec plusieurs fournisseurs, notamment F5 (F5 Aspen Mesh), Google (Anthos Service Mesh), Red Hat (OpenShift Service Mesh), Solo (Gloo Mesh), Tetrate (Tetrate Service Bridge), et VMware (Tanzu Service Mesh), qui émergent pour fournir des maillages de services basés sur Istio, soutenus par des services et un support de niveau entreprise. Istio est également proposé en tant que module complémentaire géré pour IBM Cloud.

Points forts :

En raison des efforts marketing de Google et d'IBM, « Istio » est souvent utilisé de manière interchangeable avec « service mesh », le positionnant comme la solution incontournable pour ajouter de l'observabilité, de la sécurité et de la gestion du trafic à la pile cloud native. Istio est téléchargeable gratuitement avec le support de la communauté open source. Istio est également proposé en tant que service géré par F5, Google, IBM et Red Hat pour divers environnements. Tetrate fournit une gamme complète de services de conception, de déploiement et de gestion.

Défis :

en raison de ses fonctionnalités avancées et de ses exigences de configuration complexes, Istio n'est pas aussi convivial pour l'utilisateur ou le développeur que les autres maillages de services. La réarchitecture d'Istio est en cours, avec un contrôleur multicluster centralisé, des améliorations supplémentaires pour la prise en charge des machines virtuelles et des améliorations de sécurité et de stabilité incluses dans les versions récentes. Le projet Istio ne prenant en charge que les trois dernières versions (N-2), un cycle de publication trimestriel peut s'avérer fastidieux pour les équipes dont les capacités et les compétences sont limitées.

5 – 8 - Kong : Kong Mesh- https://konghq.com/products/kong-mesh

Lancé pour une disponibilité générale en août 2020, Kong Mesh est un plan de contrôle moderne et prêt pour l'entreprise pour le maillage de services et les microservices, construit sur Envoy et Kuma, le projet open source rédigé par Kong et donné à la CNCF. Kong Mesh étend l'ensemble de fonctionnalités avancées existantes de Kuma en

incluant des fonctionnalités critiques et une prise en charge pour l'exécution des charges de travail d'entreprise. Kong Mesh fournit également des fonctionnalités de maillage de services supplémentaires et des intégrations pour la plateforme Kong Konnect, une plateforme de connectivité full-stack fournie en tant que service pour les environnements multicloud.

Une fois installé, Kong Mesh améliore la connectivité des services via des politiques qui peuvent être ajoutées à chaque maillage, service ou attribut qui qualifie un chemin de trafic, accélérant ainsi l'efficacité des développeurs, la réduction des coûts, la conformité au Règlement général sur la protection des données (RGPD) et la sécurité zéro confiance. Déployé en tant que maillage de services clé en main via une commande unique sur n'importe quel cloud, cluster Kubernetes ou infrastructure basée sur une machine virtuelle, Kong Mesh prend en charge à la fois un déploiement de plan de contrôle unique (autonome) et un déploiement multizone avec séparation du plan de contrôle global/zone.

En fait, un seul panneau de verre pour l'ensemble de l'entreprise, le plan de contrôle global agit comme le plan de contrôle principal, intégrant de nouvelles ressources et propageant automatiquement les politiques de maillage de services aux plans de contrôle de zone. Le plan de contrôle global peut être intégré aux flux de travail CI/CD existants via des CRD, une API HTTPS et la CLI de Kuma. Les plans de contrôle de zone sont déployés dans leurs zones respectives et fonctionnent comme des plans de contrôle secondaires avec un accès en lecture seule pour les proxys du plan de données dans la même zone.

La dernière version inclut des intégrations avec OPA, l'outil open source de politique en tant que code pour la prise en charge des politiques de couche 7, la configuration automatique d'Envoy pour la conformité FIPS 140-2 et l'authentification entre les plans de contrôle globaux et isolés. De plus, Kong Mesh automatise la distribution de ces politiques dans les déploiements multiclusters et multirégions, éliminant ainsi le besoin de configuration manuelle. Il étend également le maillage de services et l'OPA pour inclure les infrastructures existantes telles que les machines virtuelles.

Axé sur la facilité d'utilisation, Kong Mesh s'appuie sur Kuma pour fournir un produit multimesh pris en charge qui peut s'adapter à toutes les équipes et secteurs d'activité tout en fournissant simultanément une connectivité entre clusters et entre cloud pour les architectures modernes. Accélérant la configuration et le déploiement, Kong Mesh élimine la complexité de la configuration d'un maillage de services en encapsulant Envoy dans ses propres processus. Une interface graphique native fournit un retour visuel rapide sur ce qui se passe dans le système.

Prenant en charge les charges de travail K8 et VM, la philosophie « exécuter n'importe où » de Kong lui permet d'être déployé dans n'importe quel environnement : multicluster, multicloud et multiplateforme. Les organisations peuvent soit utiliser les

CRD de Kong Mesh pour gérer de manière native les maillages de services dans les K8, soit commencer avec un maillage de services dans les environnements de VM et migrer vers les K8 à leur propre rythme. Dans un déploiement multizone, Kong Mesh prend en charge plusieurs environnements sans augmenter la complexité. Kong propose une tarification à l'utilisation par zone, permettant aux clients d'augmenter ou de diminuer le nombre de proxys de plans de données dans la zone sans contraintes de licence.

Points forts :

La facilité d'utilisation de Kong Mesh et ses capacités d'automatisation intégrées offrent une alternative à certaines solutions open source complexes et difficiles à déployer et à gérer. Les entreprises soucieuses de leur sécurité seront attirées par la conformité FIPS 140-2 de Kong Mesh et par l'application cohérente des politiques de sécurité dans tous les environnements. L'équipe d'ingénierie de fiabilité client (CRE) de Kong offre une assistance 24h/24 et 7j/7 en utilisant un modèle de suivi du soleil conforme aux normes de l'industrie pour tous les produits Kong.

Défis :

En tant qu'entrant relativement nouveau construit sur un projet sandbox CNCF, la visualisation Kong Mesh est actuellement limitée à un plugin Grafana. Cependant, Kong développe un outil d'exploration de maillage interactif dans le cadre de son offre SMaaS. Afin de rivaliser avec succès, Kong doit ajouter des plugins WASM et un support sans serveur. De plus, en tant que leader reconnu dans le domaine des passerelles API, l'accent mis par Kong sur le maillage de services est soumis à l'adoption par les clients.

5 – 9 - Kuma (Projet CNCF)- https://kuma.io/

Créé par Kong et donné à la CNCF en tant que projet sandbox en juin 2020, Kuma est un maillage de services open source utilisant Envoy comme proxy de plan de données et un plan de contrôle développé par Kong. Conçu pour prendre en charge les applications d'entreprise nouvelles et existantes, Kuma offre une connectivité multizone évolutive sur plusieurs clusters et cloud à l'aide de systèmes nus, de K8 ou de machines virtuelles avec un proxy transparent en un clic. De plus, Kuma conserve automatiquement un inventaire de tous les side-cars proxy du plan de données exécutés dans chaque zone, permettant au maillage de services de s'adapter à n'importe quel nombre de zones et de side-cars.

Contrairement à d'autres solutions de maillage de services, Kuma fournit une prise en charge native des K8 et des VM sur les plans de contrôle et de données, avec une prise en charge multimesh dépassant les limites, y compris les espaces de noms K8. Conçu pour l'architecte d'entreprise, Kuma est livré avec une prise en charge multizone et multimesh autonome et avancée, permettant une communication entre zones entre différents clusters et cloud grâce à sa séparation globale du plan de contrôle. Un routage

flexible du trafic peut être appliqué à des zones entières, à des services individuels ou à des chemins de trafic personnalisés à l'aide de sélecteurs de source et de destination.

L'architecture de Kuma inclut une séparation des plans de contrôle, chaque zone se voyant attribuer son propre plan de contrôle évolutif horizontalement afin de minimiser la possibilité qu'une zone affecte d'autres zones en cas de panne. Le plan de contrôle global propage également automatiquement les politiques de maillage de services dans chaque zone, y compris la gestion automatisée des échecs et des rapprochements. Alors que toutes les zones sont gérées de manière centralisée via le plan de contrôle global unifié, chaque zone possède son propre plan de contrôle, qui peut également être mis à l'échelle horizontalement, afin que les politiques puissent être rapidement appliquées aux proxys du plan de données de la zone. Kuma évolue de manière linéaire et horizontale en ajoutant davantage de plans de contrôle, s'étendant jusqu'à plus de 100 000 plans de données couvrant dix zones ou plus.

Panneau de contrôle unique pour l'ensemble de l'entreprise, le plan de contrôle global peut être intégré aux flux de travail CI/CD existants via des CRD, une API HTTP ou l'interface de ligne de commande (CLI) de Kuma. Avec une architecture de politiques de couche 4 et de couche 7 prête à l'emploi permettant la découverte, l'équilibrage de charge décentralisé, l'auto-réparation automatisée, l'observabilité, le routage, la fiabilité du trafic et la sécurité zéro confiance, Kuma résume les cas d'utilisation quotidiens et propage automatiquement le service. mailler les politiques à travers l’infrastructure pour prendre en charge un environnement multimesh et multitenant sur le même plan de contrôle. De plus, la prise en charge multicloud, multicluster et multizone prête à l'emploi avec des politiques basées sur des attributs fournit une synchronisation et une connectivité automatiques des politiques pour prendre en charge les attributs de charge de travail personnalisés pour la conformité au RGPD et au secteur des cartes de paiement (PCI).

Kuma fournit des contrôles fondamentaux d'authentification, d'autorisation, de chiffrement et de stratégie couvrant les environnements, les conteneurs et les machines virtuelles. Il s'intègre nativement aux passerelles API pour prendre en charge d'autres schémas authN/authZ lors de l'exposition des services à d'autres applications, équipes ou parties externes en périphérie. Offrant une découverte de services native, Kuma prend en charge une large gamme de conteneurs, de systèmes d'exploitation et d'infrastructures cloud, chacun exécutant soit son propre maillage, soit un maillage de services hybride fonctionnant sur du bare metal, des K8 et des VM, avec une migration simplifiée entre les environnements. Facile à utiliser et ne nécessitant aucune expertise Envoy, Kuma intègre Envoy à chaque installation, injectant automatiquement le proxy side-car dans les charges de travail pour les modes de déploiement global et à distance et l'intégration native avec les solutions de gestion d'API.

Points forts :

Alors que la plupart des maillages de services donnent la priorité aux applications basées sur les K8/conteneurs, Kuma prend également en charge toutes les applications existantes exécutées sur du bare metal, des K8 ou des VM. Kuma prend en charge des clusters uniques et multiples grâce à ses options de déploiement autonomes et multizones sans augmenter la complexité du déploiement ou de la gestion. En plus d'être déployé dans des entreprises Fortune 500, Kong estime que Kuma est celui qui connaît la croissance la plus rapide de la deuxième vague de services maillés basés sur les stars publiques de GitHub. Kuma est disponible gratuitement en téléchargement sur GitHub.

Défis :

tout en prétendant remédier aux limites des technologies de maillage de services de première génération en permettant une gestion transparente de n'importe quel service sur le réseau, Kuma est un entrant relativement nouveau par rapport à d'autres maillages de services cloud natifs tels que Consul, Istio et Linkerd. Le succès de Kuma dépendra principalement de son adoption par la communauté open source et de sa promotion par Kong comme technologie sous-jacente de Kong Mesh. En tant que projet sandbox CNCF, Kuma ne fournit pas de support aux entreprises.

5 – 10 - Linkerd (Projet CNCF)- https://linkerd.io/

Le « maillage de services » original publié en 2016, **Linkerd** est un maillage de services open source hébergé par la CNCF, offrant observabilité, fiabilité et sécurité pour les applications K8 exécutées sur du métal nu ou dans le cloud sans ajouter de complexité. En tant que seul maillage de services gradué CNCF, Linkerd offre une approche ultralégère, ultrarapide et opérationnellement simple pour déployer un maillage de services sur n'importe quelle plate-forme existante. Ciblant tous les utilisateurs de K8, quelle que soit la taille de l'organisation, Linkerd s'installe en quelques minutes, ne nécessite aucune configuration et peut être ajouté progressivement à une application sans interruption. Linkerd est également livré avec des tableaux de bord Grafana et Prometheus préconfigurés et prêts à l'emploi et une prise en charge d'OpenTelemetry.

En adoptant une approche centrée sur les problèmes, la stratégie de Linkerd consiste à résoudre des problèmes immédiats et concrets – de la manière la plus générale possible – sans tenter de créer la plate-forme ultime répondant à tous les cas d'utilisation. Alors que d'autres maillages de services tendent à ajouter des fonctionnalités prenant en charge plusieurs cas d'utilisation mais nécessitant une configuration et un réglage approfondis, Linkerd se concentre sur des cas d'utilisation limités pour réduire son empreinte, automatiser autant que possible et minimiser la charge opérationnelle.

Une grande partie de la simplicité de Linkerd peut être attribuée à sa mise en œuvre du plan de données à l'aide du proxy Linkerd2 développé en interne, un « micro-proxy » réseau simple, moderne, évolutif et hautes performances basé sur Rust, plutôt que du proxy Envoy couramment utilisé. Étant donné qu’un maillage de services entièrement

déployé peut exécuter des milliers, voire des dizaines de milliers, de micro-proxys, l'impact sur la consommation de ressources et la latence s'aggrave rapidement. L'utilisation du proxy Linkerd2 permet à Linkerd de maximiser la vitesse et la sécurité du plan de données tout en optimisant la consommation des ressources. Les analyses comparatives menées par Kinvolk GmbH (une société d'ingénierie et de technologie open source récemment acquise par Microsoft) ont révélé que Linkerd était nettement plus rapide que Istio open source tout en consommant un ordre de grandeur en moins de mémoire et de processeur dans le plan de données.
En tirant parti des primitives de sécurité de K8 plutôt que d'en inventer de nouvelles, l'approche axée sur la sécurité de Linkerd est conçue pour améliorer la sécurité globale de l'environnement. Prêt pour le Zero Trust, Linkerd utilise mTLS pour fournir l'authentification de l'identité de la charge de travail, la confidentialité et l'intégrité de toutes les communications entre les pods maillés. Éliminant les vulnérabilités de sécurité communes aux projets C et C++ tels qu'Envoy, Linkerd utilise Rust comme langage de programmation du plan de données, protégeant les données sensibles des clients dans une empreinte d'exécution minimaliste tout en conservant les performances du code natif. La simplicité de Linkerd minimise le risque de mauvaise configuration ou d'évitement des fonctionnalités de sécurité en raison du coût élevé d'adoption.

En tant que créateur original de Linkerd, Buoyant a lancé Buoyant Cloud, un tableau de bord de maillage de services entièrement automatisé et unifié conçu pour surveiller, évaluer et valider la santé des clusters Linkerd. En suivant les données et les métriques du plan de contrôle, Buoyant Cloud identifie les incohérences du plan de données, gère les cycles de vie et les versions du maillage et émet des alertes de manière proactive. Le support d'entreprise pour Linkerd est disponible auprès de Buoyant et d'autres sociétés tierces.

Points forts :

Conçu dès le départ comme un maillage de services léger et axé sur la sécurité prenant en charge des fonctionnalités critiques pour les applications cloud natives utilisant K8, Linkerd est le seul maillage de services engagé dans la simplicité opérationnelle et la faible consommation de ressources. Linkerd est déployé à long terme dans des dizaines de milliers de clusters K8 dans le monde, CNCF prévoyant une adoption plus rapide que les autres maillages de services. Linkerd a une feuille de route agressive, comprenant la prise en charge récemment publiée de l'API Gateway, des politiques basées sur les routes zéro confiance, le routage dynamique des requêtes, la coupure de circuit et FIPS-140. Linkerd est disponible gratuitement en téléchargement sur GitHub.

Défis :

l'accent mis par Linkerd sur des cas d'utilisation limités peut restreindre son application à des entreprises et organisations particulières. De plus, le proxy de plan de données de Linkerd ne prend actuellement en charge que les charges de travail K8 exécutées sur du bare metal ou dans le cloud. Le support de Linkerd est principalement fourni par la

communauté open source. Cependant, le créateur de Linkerd, Buoyant, et d'autres sociétés tierces proposent une assistance payante aux entreprises clientes.

5 – 11 - NSM – Network Service Mesh - https://networkservicemesh.io/

Donné à la CNCF en avril 2019**, Network Service Mesh (NSM)** est un **projet de bac à sable** communautaire qui prend rapidement de l'ampleur en raison de sa capacité à simplifier la connectivité entre les charges de travail, quel que soit l'endroit où elles s'exécutent. En tant que maillage de services IP hybride et multicloud, NSM étend l'accessibilité IP aux charges de travail exécutées sur site, dans des environnements existants, sur plusieurs clusters et dans des cloud publics, en communiquant à l'aide des protocoles existants. De plus, étant donné que les charges de travail individuelles n'ont besoin d'une connectivité qu'à une sélection limitée d'autres charges de travail, NSM fournit une connectivité IP hybride et multicloud pour les applications et les maillages de services d'application sans nécessiter aucune modification.

Construit à partir de zéro, NSM fait passer le réseau IP de l'infrastructure à une sélection de services réseau. En connectant une charge de travail individuelle (ou pod K8s) à un service réseau via un simple ensemble d'API, NSM permet à l'infrastructure de rester immuable tout en répondant à une grande variété d'exigences. NSM permet également aux charges de travail individuelles de se connecter à un service réseau via un WireGuard vWire injecté dans le pod en tant qu'interface secondaire non conflictuelle. Enfin, en faisant correspondre la sélection des services réseau à la granularité de la charge de travail plutôt qu'au cluster, NSM permet à différentes charges de travail de consommer des services réseau différents, potentiellement conflictuels.

En tant que couche d'infrastructure supplémentaire fonctionnant au-dessus des K8 prêts à l'emploi, NSM mappe le concept de maillage de services des charges de travail de couche 7 aux charges de travail de couche 2 et 3, offrant ainsi une connectivité, une observabilité et une sécurité supplémentaires au niveau des couches réseau. . En complétant les maillages de services d'application de niveau supérieur en les traitant comme faisant partie d'un service réseau, un maillage de services Consul, Istio, Linkerd ou autre peut s'exécuter comme une instance unique au-dessus de la couche 3 virtuelle de NSM couvrant plusieurs clusters, cloud ou organisations.

NSM associe de manière lâche les charges de travail aux services réseau pertinents indépendamment de l'environnement sous-jacent, permettant aux charges de travail individuelles de rejoindre simultanément plusieurs services réseau, chaque service réseau ayant son propre plan de contrôle segmenté selon les lignes logiques du service. En conséquence, le maillage de services offre la simplicité opérationnelle d'une solution de cluster unique tout en permettant aux charges de travail exécutées dans plusieurs clusters sur plusieurs cloud de se connecter via un service réseau partagé, quel que soit leur emplacement.

Lorsqu'il est installé sur un cluster K8s, NSM simplifie la connectivité réseau sophistiquée pour le développeur. Conçus pour fonctionner à l'échelle d'Internet, les points de terminaison de services réseau exécutés n'importe où peuvent annoncer des services réseau dans un domaine de registre de services réseau. À son tour, NSM permet à toute charge de travail autorisée, située n'importe où, de demander un service réseau publié à partir d'un ou plusieurs registres de services. Aucune modification n'est apportée aux K8 ou au plug-in CNI utilisé.

En plus de fonctionner sur du matériel nu, NSM a été testé avec Amazon EKS, GKE, Microsoft Azure Kubernetes Service (AKS) et sur des clusters publics. NSM est géré via une CLI et des API gRPC bien définies pour l'enregistrement des services réseau et des points de terminaison des services réseau auprès de son serveur de registre. NSM inclut également des capacités d'auto-réparation, utilise OPA pour appliquer des politiques d'admission basées sur les identités SPIFF et SPIRE, et s'intègre à Prometheus et OpenTelemetry pour l'observabilité. (Remarque : SPIRE est une implémentation de SPIFFE prête pour la production.)

Points forts :

Network Service Mesh est le seul maillage de services fonctionnant sur les charges de travail de couches 2 et 3. Adopté par Cisco, Ericsson et Intel pour les architectures de nouvelle génération, NSM complète les maillages de services de couche 7 en offrant une connectivité, une observabilité et une sécurité supplémentaires. De plus, Ericsson contribue activement à NSM pour permettre des cas d'utilisation spécifiques à la 5G pour les fonctions réseau natives du cloud. Network Service Mesh est disponible gratuitement en téléchargement sur GitHub.

Défis :

Bien que NSM offre des avantages tangibles et suscite un intérêt considérable de la part des principaux acteurs du secteur, il manque d'adoption généralisée. Cependant, avec plusieurs solutions basées sur NSM destinées à être déployées en direct, nous prévoyons une augmentation de leur adoption.

5 – 12 - Red Hat : Mesh de services OpenShift -

https://www.redhat.com/fr/technologies/cloud-computing/openshift/what-is-openshift-service-mesh

Annoncé en août 2019, **Red Hat OpenShift** Service Mesh (**OSSM**) offre un moyen uniforme de connecter, gérer et observer les applications basées sur des microservices exécutées au sein d'OpenShift Container Platform, un PaaS privé développé par Red Hat pour les entreprises exécutant OpenShift sur site. ou une infrastructure de cloud public. Basé sur le projet open source Istio, OSSM fournit des informations comportementales et un contrôle opérationnel de Maistra Service Mesh, une distribution avisée d'Istio conçue pour fonctionner avec OpenShift. OpenShift Service Mesh regroupe Maistra Service Mesh, intégrant des fonctionnalités spécifiques d'Istio utilisant le proxy Envoy,

avec Jaeger et Kiali dans une plate-forme offrant la découverte, l'authentification de service à service, l'équilibrage de charge, la reprise après panne, les métriques et la surveillance.

Conçu pour être prêt pour la production, OSSM augmente la productivité des développeurs et accélère le délai de rentabilisation des applications en intégrant des communications de service à service basées sur des politiques sans modifier le code de l'application ni intégrer de bibliothèques spécifiques au langage. Testé avec d'autres produits Red Hat, OSSM s'installe facilement sur Red Hat OpenShift et est livré avec un support de niveau entreprise, simplifiant et rationalisant la gestion du personnel d'exploitation.

OSSM utilise Grafana, Jaeger, Kiali et une sécurité prête à l'emploi pour tracer, observer et sécuriser les communications intra-service. Plateforme d'observabilité et de visualisation de données ouverte, composable et interactive, Grafana permet aux utilisateurs d'interroger, de visualiser, de comprendre et de déclencher des alertes pour les métriques, quel que soit l'endroit où elles sont stockées. Jaeger, un système de traçage distribué open source de bout en bout, surveille et dépanne les transactions dans les systèmes distribués complexes. Facultatif mais installé par défaut, Jaeger permet aux utilisateurs de suivre une seule demande au fur et à mesure de son cheminement entre différents services, ou même à l'intérieur d'un service, offrant ainsi un aperçu de l'ensemble du processus de demande du début à la fin.

La console de gestion pour OSSM, Kiali, un autre projet open source, est spécialement conçue pour configurer, valider, visualiser, surveiller et dépanner les maillages de services Istio en temps quasi réel afin d'augmenter la disponibilité et les performances. Offrant une vue intuitive de bout en bout de tous les microservices, Kiali affiche la structure du maillage de services en déduisant la topologie du trafic et en utilisant des métriques de service pour indiquer l'état, la fiabilité et les performances des applications, offrant ainsi une visibilité sur des fonctionnalités telles que les disjoncteurs et les demandes. les taux. De plus, Kiali s'intègre à Jaeger pour dépanner et isoler les goulots d'étranglement dans les chemins de requêtes de bout en bout.

Fournissant une sécurité prête à l'emploi pour les applications distribuées, OSSM connecte en toute sécurité les services par défaut à l'aide d'un cryptage mTLS transparent et applique un modèle de sécurité réseau zéro confiance avec des politiques de trafic précises basées sur les identités des applications. De plus, le maillage de services offre des capacités de gestion du trafic pour faciliter les basculements, les déploiements Canary, la mise en miroir du trafic et les tests A/B. En contrôlant le flux de trafic et les appels API entre les services, OSSM améliore la fiabilité des services grâce à des tentatives de requêtes automatiques, des délais d'attente et des disjoncteurs, rendant les applications plus résilientes.

Contrairement aux déploiements Istio en amont, OSSM offre des fonctionnalités pour faciliter le déploiement sur Red Hat OpenShift et aider à résoudre les problèmes, notamment l'installation d'un plan de contrôle mutualisé, l'extension des fonctionnalités RBAC, le remplacement de BoringSSL (un dérivé d'OpenSSL) par OpenSSL et l'activation de Kiali et Jaeger en défaut. Plutôt que d'injecter automatiquement des side-cars Envoy dans les pods K8, OSSM nécessite une annotation, offrant plus de contrôle en permettant aux utilisateurs de sélectionner les services à inclure dans le maillage. OSSM a récemment ajouté la prise en charge de l'API Kubernetes Gateway, d'une console OpenShift Service Mesh et d'une option de topologie à l'échelle du cluster cohérente avec la topologie de déploiement d'Istio en amont.

Points forts :
OSSM fournit un moyen uniforme de connecter, gérer et observer les applications basées sur des microservices exécutées dans un environnement Red Hat OpenShift. Conçu pour s'intégrer à d'autres produits Red Hat, OSSM s'installe facilement sur Red Hat OpenShift et inclut un support de niveau entreprise, simplifiant et rationalisant la gestion du personnel d'exploitation. OSSM est disponible gratuitement pour les utilisateurs d'OpenShift à partir du catalogue Red Hat Ecosystem.

Défis :
Le Maistra Service Mesh sous-jacent d'OSSM est un clone d'Istio et est en retard par rapport aux versions parentes d'Istio. Cependant, RedHat a commencé à travailler sur une version majeure dans le but de faire converger OSSM avec la communauté Istio pour une compatibilité accrue et un développement plus rapide. OSSM ne prend pas en charge les machines virtuelles. De plus, bien que OSSM ne prenne pas en charge les mises à niveau Canary du plan de contrôle, il utilise l'opérateur OpenShift Service Mesh pour l'installation et les mises à niveau.

5 – 13 - Solo.io : Gloo Mesh- https://www.solo.io/products/gloo-mesh/

Lancé début 2019, **Gloo Mesh** est un plan de contrôle moderne natif K8 permettant la configuration et la gestion opérationnelle de plusieurs maillages de services hétérogènes sur plusieurs clusters via une API unifiée. Conçu pour remplacer tout environnement Istio existant, Gloo Mesh peut être exécuté soit dans son propre cluster, soit colocalisé avec un maillage existant, permettant le routage global du trafic, l'équilibrage de charge, le contrôle d'accès et l'observabilité centralisée des environnements multiclusters. Il découvre les maillages et les charges de travail et établit une identité fédérée, facilitant la configuration de différents maillages de services via une seule API.

Version améliorée d'Istio open source (par opposition à un fork), Gloo Mesh Enterprise inclut une version étendue du proxy Envoy. Cette fonctionnalité permet une configuration et une orchestration cohérentes des services sur plusieurs machines virtuelles, clusters, cloud et centres de données à partir d'un seul point de contrôle. En se concentrant sur la facilité d'utilisation, Gloo Mesh Enterprise valide le logiciel Istio en

amont et intègre les meilleures pratiques intégrées en matière d'extensibilité et de sécurité, y compris des API basées sur les rôles.

Gloo Mesh Enterprise comprend un maillage de services basé sur Istio compatible FIPS 140-2 avec un service automatisé et une découverte d'API appliquant une sécurité zéro confiance avec authentification, autorisation et cryptage. La passerelle Gloo Mesh offre un cryptage, une sécurité et un contrôle du trafic de bout en bout, intégrant la gestion du trafic dans les flux de transfert de données est/ouest et nord/sud. De plus, les extensions Gloo Mesh permettent aux clients d'étendre et de personnaliser leur infrastructure API avec des extensions et des outils prédéfinis pour WebAssembly, des plug-ins et des opérateurs, étendant ainsi les capacités de proxy Envoy personnalisées. Un portail en libre-service permet aux développeurs de cataloguer, publier et partager des API dans un environnement sécurisé.

Gloo Mesh prend en charge Istio Ambient Mesh (co-développé par Solo et Google), une nouvelle architecture de plan de données Istio sans side-car offrant des opérations simplifiées, une compatibilité d'application plus large et des coûts réduits. Alternative aux side-cars Envoy, Istio Ambient Mesh divise les fonctionnalités d'Istio en une couche de superposition sécurisée et une couche de traitement de couche 7, chacune offrant des capacités pertinentes de télémétrie, de gestion du trafic et de sécurité zéro confiance. Entièrement interopérable avec les déploiements side-car, l'approche en couches d'Ambient Mesh permet aux utilisateurs d'adopter Istio progressivement par espace de noms, en passant d'abord à une superposition sécurisée avant de mettre en œuvre un traitement complet de couche 7.

Fournissant une interface unique pour la mise en réseau d'applications cloud natives, Gloo Platform est la plate-forme complète de mise en réseau d'applications de Solo, comprenant Gloo Mesh, Gloo Gateway (API-GW), Gloo Network (Cilium CNI) et Gloo Fabric (Multi-Cloud). Bien que les composants puissent être achetés et déployés individuellement, ils sont intégrés à un seul plan de contrôle unifié, un plan de gestion unifié et une API pour le provisionnement. L'API Gloo Mesh s'intègre aux principaux maillages de services et élimine les différences entre leurs API disparates, rationalisant ainsi la configuration, le fonctionnement et la gestion du cycle de vie des environnements multicloud, multimesh et multitenant.

De plus, une extension de Gloo Platform, Gloo Fabric, permet de regrouper les applications exécutées sur des conteneurs, des machines virtuelles ou un calcul sans serveur dans un espace de travail cloud virtuel sécurisé et isolé pour accélérer les migrations d'applications ou gérer des applications couvrant plusieurs environnements. En tant que plan de contrôle découplé pour le proxy Envoy, Gloo Edge permet aux clients d'ajouter de manière itérative des capacités de maillage de services à l'entrée de leur cluster sans investir dans un maillage de services à part entière. Solo.io propose également Gloo GraphQL, la seule implémentation du secteur du moteur GraphQL intégré à Envoy.

Points forts :

Gloo Mesh Enterprise est un maillage de services et un plan de gestion basés sur Istio qui simplifie et unifie la configuration, le fonctionnement et la visibilité de la connectivité service à service au sein des applications distribuées. Solo.io propose des distributions améliorées d'Istio open source en amont (y compris FIPS, ARM, LTS) et Envoy Proxy, un support de production et une gestion simplifiée et centralisée du cycle de vie d'Istio et d'Envoy pour les environnements greenfield et brownfield. Solo.io est le premier fournisseur à prendre en charge Istio Ambient Mesh, offrant une alternative sans side-car pour Gloo Mesh Enterprise. Solo.io propose un modèle d'abonnement basé sur un cluster. Une distribution open source gratuite est également disponible.

Défis :

Avec toutes les options disponibles, le portefeuille de produits de Solo.io peut être déroutant et difficile à naviguer. Bien qu'il contribue aux projets Istio et Envoy et qu'il investisse massivement dans le talent et l'innovation, Solo.io dépend toujours d'Envoy et d'Istio open source pour ses offres de base. Et bien que Solo.io offre une prise en charge étendue d'Istio, les actualisations périodiques forcées peuvent potentiellement être perturbées. Cependant, avec le transfert d'Istio à la CNCF, Solo.io dispose de 3 sièges sur 6 au sein du comité de surveillance technique d'Istio, ce qui offre la possibilité d'affirmer son autorité et de prendre les devants pour influencer la direction d'Istio.

5 – 14 - Traefik Mesh Labs- https://traefik.io/traefik-mesh/

Lancé en septembre 2019 et précédemment connu sous le nom de Maesh**, Traefik Mesh** est un maillage de services simple, direct et non invasif utilisant Traefik Proxy (plutôt qu'Envoy) pour gérer les communications de service à service au sein d'un cluster K8. Créé et maintenu principalement par Traefik Labs (anciennement Containous), Traefik Proxy est l'un des proxys d'applications cloud natifs les plus utilisés, avec plus de 3 milliards de téléchargements et plus de 44 000 étoiles GitHub. Traefik Labs affirme que Traefik Mesh est le maillage de services le plus simple et le plus facile à déployer pour un contrôle, une sécurité et une observabilité améliorés sur tous les flux de trafic est/ouest avec une surcharge minimale.

S'intégrant nativement aux K8, Traefik Mesh est un maillage de services léger mais complet prenant en charge la dernière spécification SMI. Traefik Mesh prend en charge une architecture par nœud au lieu d'un proxy side-car pour plus de simplicité et de conservation des ressources. Étant donné que Traefik Mesh est opt-in par défaut, les services existants ne sont pas affectés jusqu'à ce qu'ils soient explicitement ajoutés au maillage de services plutôt que d'être automatiquement injectés dans l'application.

Étant donné que Traefik Mesh n'utilise aucun conteneur side-car, le routage est géré via des points de terminaison proxy sur chaque nœud. Tirant parti des points de terminaison de Traefik Mesh, l'architecture sans side-car signifie que Traefik Mesh ne modifie pas

les objets ou le trafic de K8 à l'insu de l'utilisateur. Prenant en charge plusieurs options de configuration, y compris les annotations sur les objets de service utilisateur et les objets SMI, le contrôleur de maillage s'exécute dans un pod dédié et gère toute l'analyse de la configuration et le déploiement sur les nœuds proxy.

Conçu pour la simplicité en mettant l'accent sur l'efficacité et la faible utilisation des ressources, Traefik Mesh est facile à installer et à configurer via une CLI. Son ensemble de fonctionnalités comprend des capacités de gestion du trafic, telles que des disjoncteurs, l'équilibrage de charge, les tentatives et les basculements, ainsi que la limitation du débit. De plus, Traefik Mesh offre une observabilité avec des métriques prêtes à l'emploi préinstallées avec Grafana et Prometheus et est compatible avec Datadog, InfluxData et StatsD. Le traçage est fourni via OpenTelemetry, offrant une compatibilité totale avec Haystack, Instana, Jaeger et Zipkin pour un traçage et une analyse résilients et évolutifs.

En plus de la sécurité de base sous forme de mTLS, Traefik Mesh est compatible SMI et facilite le réglage fin des autorisations de trafic via le contrôle d'accès. Spécification pour les maillages de services fonctionnant sur K8, SMI définit une norme commune pour les fournisseurs de maillages de services, couvrant les capacités les plus courantes et permettant la flexibilité et l'interopérabilité. De plus, étant donné que SMI est spécifié comme un ensemble d'API K8, les utilisateurs qui connaissent les K8 peuvent utiliser Traefik Mesh.

Construit sur Traefik Proxy et Traefik Mesh open source, Traefik Enterprise consolide la passerelle API, le contrôle d'entrée et le maillage de services dans un seul plan de contrôle simple. Solution de connectivité unifiée et native du cloud, Traefik Enterprise simplifie la complexité de la mise en réseau des microservices avec des fonctionnalités distribuées, hautement disponibles et évolutives combinées à une prise en charge groupée premium par abonnement pour les déploiements de niveau entreprise. De plus, Traefik Enterprise comprend un tableau de bord amélioré avec une observabilité du maillage de services du trafic interne est/ouest.

Points forts :

Traefik Mesh comprend une sélection de fonctionnalités pour obtenir une bonne convivialité et de bonnes performances, notamment des disjoncteurs, l'équilibrage de charge, la limitation de débit, les tentatives et les basculements, et la sécurité, ainsi que l'observabilité et les métriques prêtes à l'emploi. Utilisant le populaire Traefik Proxy, Traefik Mesh offre une gestion du trafic légère, conforme à SMI et non invasive avec une bonne convivialité et de bonnes performances. Au lieu d'un proxy side-car, Traefik Mesh utilise des services de connexion proxy par nœud opt-in, offrant un contrôle accru tout en minimisant la consommation de ressources. Traefik Mesh inclut un support communautaire open source ou un support d'entreprise par abonnement de Traefik Labs.

Défis :

Traefik Mesh ne dispose pas de fonctionnalités multicluster. Les utilisateurs ayant besoin d'un plan de contrôle unifié couvrant les clusters, les nuages et les maillages devraient donc chercher ailleurs. Bien que Traefik Mesh prenne en charge le contrôle d'accès SMI, il n'offre pas de cryptage transparent de bout en bout et ne prend pas en charge les machines virtuelles.

5 – 15 - VMware : Tanzu Service Mesh- https://tanzu.vmware.com/fr/service-mesh

Annoncé en décembre 2018 sous le nom de NSX Service Mesh et lancé sous le nom de **Tanzu Service Mesh (TSM)** en mars 2020, TSM est un maillage de services de classe entreprise basé sur Istio offrant une connectivité et une sécurité cohérentes pour les microservices dans les environnements K8 multiclusters et multicloud. TSM s'intègre à Tanzu Mission Control (TMC) dans un modèle faiblement couplé pour fournir des fonctionnalités de maillage de services standard via l'API Istio. TSM prend également en charge Tanzu Kubernetes Grid et la plate-forme K8s de **VMware**, en plus d'AKS, EKS, GKE, OpenShift et d'autres distributions K8s pour créer un maillage de services multiplateforme. TSM propose une prise en charge unique de cas d'utilisation de bout en bout et des solutions intégrées difficiles à réaliser avec les seules technologies de maillage de services. Exploité en mode SaaS, le contrôleur global de TSM est une solution entièrement gérée, exploitée et maintenue par VMware.
Tanzu Service Mesh comprend le contrôleur global TSM (un plan de contrôle fourni sous forme de SaaS géré par VMware) et le plan de données TSM exécuté sur les clusters K8 des clients. Basé sur Istio et Envoy open source, le plan de données TSM fournit des services typiques tels que l'authentification et l'autorisation, la coupure de circuit, la limitation de débit, les délais d'attente et les tentatives, le transfert de trafic et d'autres fonctionnalités. Le plan de données TSM comprend également l'agent TSM, qui fournit une connexion sécurisée entre les clusters des clients et le contrôleur global TSM pour gérer la configuration et les stratégies appliquées dans le plan de données TSM.

Tanzu Service Mesh comprend une couche d'abstraction d'application unique appelée Global Namespace (GNS), qui agit comme un regroupement logique pour les microservices. Gérés via un modèle d'API déclaratif et une interface utilisateur intuitive, les GNS fournissent aux applications modernes une configurabilité simplifiée, une automatisation basée sur l'API, une isolation et une cohérence opérationnelle pour DevOps et la sécurité, quelle que soit la plate-forme ou le cloud sous-jacent. Ils fournissent également des services automatisés de découverte et de dénomination (DNS), de politiques de résilience, de politiques de sécurité, de graphiques de services et de routage du trafic.

Permettant l'automatisation complète des configurations multiclusters (dans un modèle fédéré où le plan de contrôle de chaque cluster est indépendant et le trafic inter-clusters est limité au plan de données), les configurations d'entrée et de sortie et la portabilité transparente des applications inter-cloud, GNS prend en charge les microservices au

sein d'un seul et même système. cluster et microservices distribués sur plusieurs clusters et cloud. L'intégration avec Tanzu Application Platform (TAP) offre une expérience de développement améliorée, permettant de préconfigurer la connectivité, la résilience et l'intention de sécurité dans un GNS, puis de les déployer automatiquement sur les applications TAP.

TSM offre une gestion complète du cycle de vie du maillage de services avec une intégration automatisée du cluster lors de l'installation d'Istio ; opérations en un clic pour mettre à niveau, corriger, restaurer ou supprimer le plan de données TSM des clusters sur n'importe quelle plate-forme K8 ou environnement cloud ; et des contrôles et une gestion automatisés de l'état du plan de données pour minimiser la dérive de configuration. TSM fonctionne soit de manière autonome, soit dans le cadre d'un workflow de gestion du cycle de vie entièrement intégré géré par TMC. De plus, TSM fonctionne avec NSX Advanced Load Balancer de VMware (anciennement Avi Networks) pour fournir une prise en charge multicloud, des politiques unifiées, un équilibrage de charge, une entrée, une mise en réseau de conteneurs et une observabilité dans les environnements VMware et K8 tiers.

La sécurité contextuelle des API (basée sur l'acquisition de Mesh7 par VMware en mars 2021) permet aux développeurs et aux équipes de sécurité de mieux comprendre quand, où et comment les applications et les microservices communiquent via les API, même dans des environnements multicloud, permettant ainsi un meilleur DevSecOps. Intel et VMware travaillent également ensemble pour optimiser et accélérer le middleware et l'infrastructure des microservices avec des logiciels, notamment eBPF, en mettant l'accent sur l'amélioration des performances, les accélérations de chiffrement et la sécurité pour la création de charges de travail distribuées.

Points forts :

S'appuyant sur Istio open source, Tanzu Service Mesh fournit des services d'entreprise robustes, y compris la mise à l'échelle automatique, sur plusieurs clusters K8, offrant une simplification et une automatisation opérationnelles avec des fonctions avancées de résilience et de sécurité. En plus de prendre en charge diverses plates-formes d'applications, cloud publics et environnements d'exécution, Tanzu Service Mesh prend en charge la fédération sur plusieurs clusters pour une connectivité, une résilience et une sécurité de bout en bout. VMware propose un modèle d'abonnement principal par nœud Kubernetes avec support de production inclus.

Défis :

Bien qu'il soit capable de fonctionner de manière totalement indépendante de la pile technologique de VMware, Tanzu Service Mesh offre une valeur accrue à la base installée de VMware plutôt qu'à un public plus large. TSM manque actuellement de capacités de sécurité de bout en bout, y compris l'extensibilité de TSM aux solutions tierces et VMware de détection et de réponse des points de terminaison (EDR) et de gestion des appareils mobiles (MDM), y compris VMware Carbon Black. TSM

comprend plusieurs technologies de passerelle et d'équilibrage de charge qui se chevauchent, ce qui présente des défis de configuration.

Annexe : Bibliographie

1 – reference

- https://gigaom.com/reprint/gigaom-radar-for-service-mesh-237742-kong/

2 - À propos de GigaOm

GigaOm fournit des conseils techniques, opérationnels et commerciaux pour l'entreprise numérique stratégique et les initiatives commerciales. Les chefs d'entreprise, les DSI et les organisations technologiques s'associent à GigaOm pour obtenir des conseils pratiques, exploitables, stratégiques et visionnaires pour moderniser et transformer leur entreprise. Les conseils de GigaOm permettent aux entreprises de rivaliser avec succès dans un environnement commercial de plus en plus complexe qui nécessite une solide compréhension des demandes des clients en constante évolution.

GigaOm travaille directement avec les entreprises à l'intérieur et à l'extérieur de l'organisation informatique pour appliquer des recherches et des méthodologies éprouvées conçues pour éviter les pièges et les obstacles tout en équilibrant risque et innovation. Les méthodologies de recherche comprennent, sans s'y limiter, des enquêtes d'adoption et d'analyse comparative, des cas d'utilisation, des entretiens, le retour sur investissement/coût total de possession, les paysages du marché, les tendances stratégiques et les références techniques. Nos analystes possèdent plus de 20 ans d'expérience dans le conseil à un large éventail de clients, des premiers utilisateurs aux grandes entreprises.

Le point de vue de GigaOm est celui d'un praticien impartial en entreprise. Grâce à cette perspective, GigaOm se connecte avec des abonnés engagés et fidèles à un niveau profond et significatif.

3 – A propos de CNCF

La Cloud Native Computing Foundation (CNCF) est une organisation à but non lucratif qui favorise la croissance des technologies cloud natives. Voici un aperçu de ce qu'ils font :

- Open Source et neutre vis-à-vis des fournisseurs : La CNCF crée un environnement open source et neutre vis-à-vis des fournisseurs où différentes entreprises peuvent collaborer sur des projets cloud natifs. Cela favorise l'innovation et garantit que les technologies ne sont pas contrôlées par un seul fournisseur.

- Soutient les projets clés : Ils fournissent un soutien et une orientation pour les projets cloud natifs critiques, notamment :

    - **Kubernetes** : plateforme d'orchestration de conteneurs utilisée pour automatiser le déploiement, la mise à l'échelle et la gestion des applications conteneurisées.

    - **Prometheus** : un système de surveillance pour la collecte et l'analyse des données provenant d'applications cloud natives.
    - **Envoy** : un proxy et un équilibreur de charge hautes performances pour les microservices cloud natifs.
- Écosystème cloud natif élargi : La CNCF va au-delà de ces projets populaires. Ils disposent d'une grande collection (plus de 180 !) d'autres projets cloud natifs à différents stades de développement, classés comme incubateurs ou gradués en fonction de leur maturité.

- Renforcement de la communauté : Ils encouragent une communauté collaborative autour des technologies cloud natives. Cela inclut l'organisation de conférences telles que KubeCon et CloudNativeCon, où les développeurs, les utilisateurs et les fournisseurs peuvent se réunir pour partager des connaissances et des idées.

En résumé, la Cloud Native Computing Foundation joue un rôle central dans la définition, le développement et la promotion des technologies cloud natives. Leur travail est essentiel à la création et à l'exécution d'applications modernes et évolutives.