RAPPORT DE MARCHÉ

Rapport GigaOm sur l’observabilité cloud v1.0

ANDY THURAI | 26 FÉVR. 2021 – 10h57 (CST)

SUJET : INFRASTRUCTURE CLOUD

CRÉDIT : BAGOTAJ

GIGAOM

Rapport GigaOm sur l’observabilité cloud

TABLE DES MATIÈRES

1. Résumé

L'observabilité est un nouvel ensemble de pratiques, de plates-formes et d'outils qui vont au-delà de la surveillance pour fournir des informations sur l'état interne des systèmes en analysant les résultats externes. Il s'agit d'un concept qui a ses racines dans les principes de la théorie du contrôle du XIXe siècle et qui gagne aujourd'hui rapidement du terrain.

Il est indéniable que la surveillance représente une fonction essentielle de l'informatique depuis des décennies. Toutefois, les approches traditionnelles sont devenues inadaptées pour diverses raisons, entre autres, les déploiements cloud, la méthodologie de développement agile, les déploiements continus et les nouvelles pratiques DevOps. Ces changements ont modifié la façon dont les systèmes, l'infrastructure et les applications doivent être observés pour que les événements et les incidents puissent être rapidement pris en compte.

Le concept d'observabilité repose sur un principe fondamental : apprenez rapidement ce qui se passe au sein de votre service informatique pour éviter des interruptions prolongées. Et dans l'éventualité d'une interruption, vous devez vous assurer que vous pouvez identifier rapidement la cause première de cette interruption. Les interruptions sont mesurées par le délai moyen de résolution et l'objectif du concept d'observabilité est de réduire au maximum ce délai.

Il n'est donc pas surprenant que la mise en place de systèmes de diffusion de services robustes et hautement disponibles constitue l'objectif ultime pour toute entreprise. Pour atteindre cet objectif, trois concepts clés doivent être exécutés :

- **Surveillance :** il s'agit de comprendre si les processus fonctionnent correctement dans une optique de service.
- **Observabilité :** il s'agit d'offrir une visibilité complète de bout en bout de vos applications, systèmes, API, microservices, réseau, infrastructure, et plus encore.
- **AIOps (Artificial Intelligence for IT Operations ou Intelligence artificielle pour les opérations informatiques) :** il s'agit d'utiliser cette visibilité complète pour tirer un sens des données collectées afin de produire des informations exploitables et des plans d'action.

Pour atteindre les objectifs d'observabilité, vous devez mesurer les signaux clés de télémétrie : journaux, métriques et traces. Les journaux et les métriques sont mesurés par les professionnels de l'informatique depuis des décennies. Cependant, les traces constituent un concept assez nouveau qui a émergé au fur et à mesure du développement des applications modernes à l'aide de microservices distribués. Une demande de service n'est plus traitée par un service, mais plutôt par une composition de microservices, et il est donc impératif de suivre ou de tracer la demande de service du début à la fin. Afin de générer une télémétrie appropriée, tous les systèmes sous-jacents doivent être correctement instrumentés. Ainsi, les entreprises peuvent obtenir une visibilité complète de leurs systèmes pour suivre les appels de service, identifier les interruptions et déterminer si les systèmes affectés se trouvent sur site, dans le cloud ou ailleurs.

L'observabilité ne consiste pas toujours à introduire de nouveaux outils, mais à consolider les données de télémétrie, à instrumenter correctement les systèmes pour obtenir la télémétrie appropriée, à créer des informations exploitables, ainsi qu'à éviter les interruptions prolongées. L'observabilité complète est essentielle pour assurer la pérennité de l'infrastructure informatique.

Ce rapport évalue les principaux fournisseurs du nouveau marché de l'observabilité des applications/systèmes/infrastructures et vise à fournir aux décisionnaires informatiques les informations dont ils ont besoin pour sélectionner les fournisseurs en fonction de leurs besoins spécifiques. Nous avons analysé les fournisseurs sur un ensemble de critères clés et de métriques d'évaluation, qui sont décrites en détail dans le rapport « Key Criteria Report for Cloud Observability » (Rapport sur les critères clés de l'observabilité cloud).

COMMENT LIRE CE RAPPORT

Ce rapport GigaOm fait partie d'une série de documents qui aident les services informatiques à évaluer les solutions concurrentes selon des caractéristiques et des critères bien définis. Pour en savoir plus, veuillez consulter les rapports suivants :

Rapport sur les critères clés : analyse de marché détaillée qui évalue l'impact des fonctionnalités et critères clés du produit sur les caractéristiques globales de la solution (telles que l'évolutivité, les performances et le coût total de possession) qui influencent les décisions d'achat.

Rapport GigaOm : analyse prospective qui mesure la valeur relative et la progression des solutions de fournisseurs sur plusieurs axes, en fonction de la stratégie et de l'exécution. Ce rapport inclut une analyse détaillée de l'offre de chaque fournisseur du secteur.

Profil du fournisseur : analyse approfondie des fournisseurs qui s'appuie sur le cadre élaboré dans le rapport sur les critères clés et le rapport GigaOm pour évaluer l'engagement d'une entreprise dans un secteur technologique. Cette analyse comprend des recommandations prospectives aussi bien en termes de stratégie comme de produit.

2. Catégories de marché et types de déploiement

Pour mieux comprendre le marché et le positionnement des fournisseurs (**Tableau 1**), nous allons évaluer la capacité des solutions d'observabilité cloud à répondre aux besoins de secteurs d'activité spécifiques.

Type de déploiement

Les outils d'observabilité sont généralement fournis dans les modèles de déploiement et de consommation suivants :

Modèle SaaS public
La plate-forme est gérée par les fournisseurs sur des sites de cloud public (AWS, GCP ou Azure) et proposée sous forme d'offre SaaS aux utilisateurs. Elle est accessible directement via un portail Web sans installation supplémentaire. Souvent considéré comme le chemin le plus simple vers l'observabilité, le modèle SaaS public représente la norme de facto pour le déploiement de la plate-forme d'observabilité chez la plupart des fournisseurs.

Modèle SaaS privé
Il s'agit d'une variante du modèle SaaS public : les fournisseurs du modèle SaaS privé proposent leurs solutions d'observabilité sous forme de plates-formes SaaS hébergées et mutualisées à partir de leurs propres centres de données. Bien que cette approche offre la plupart des fonctionnalités disponibles dans le SaaS public, certaines fonctionnalités cloud natives peuvent manquer, par exemple, la prise en charge de l'accès sans serveur et la disponibilité d'outils supplémentaires dans le cloud public.

Logiciel sur site
Certains fournisseurs proposent aux entreprises d'installer, de configurer et de gérer elles-mêmes la solution sur des sites de cloud privé (sur site, par exemple). Si cette option peut être intéressante notamment pour des clients qui placent la sécurité et la conformité au premier plan, elle peut s'avérer moins flexible en termes d'utilisation et ne pas disposer de fonctionnalités cloud natives.

Instrumentation et ouverture

Ouverture
Certains fournisseurs d'observabilité proposent des solutions Open Source ou à licence ouverte gratuites dotées de puissantes fonctionnalités complémentaires. La solution proposée par Elastic qui repose sur la pile ELK (Elasticsearch, Logstash, Kibana) en est d'ailleurs un bon exemple. D'autres fournisseurs offrent une combinaison d'intégrations Open Source pour concevoir des mises en œuvre de premier ordre pensées pour les entreprises qui améliorent la sécurité, l'évolutivité, la facilité de gestion, la gouvernance et d'autres fonctionnalités encore. Logz.io, par exemple, repose sur la pile ELK tout en intégrant Prometheus et Grafana, ainsi que Jaeger pour le traçage distribué.

Instrumentation

Dans ce domaine, les variantes sont nombreuses. Certains fournisseurs exigent l'installation d'outils d'instrumentation pour collecter la télémétrie. La plupart du temps, ce processus est manuel et peut être chronophage, surtout lorsqu'il est associé à des microservices distribués. D'autres fournisseurs offrent des fonctions d'instrumentation automatique ou en un clic qui peuvent faciliter le processus. Enfin, certains fournisseurs proposent une intégration avec des outils Open Source tels que FluentD et Prometheus. Ces options offrent toutes différents niveaux d'ouverture et de flexibilité.

OpenTelemetry

L'initiative OpenTelemetry fournit une infrastructure d'observabilité Open Source pour les logiciels cloud natifs qui se développe rapidement afin d'inclure des normes ouvertes pour les journaux, les métriques et les traces. Cette infrastructure est de plus en plus adoptée par les géants du cloud, tandis que les fournisseurs d'observabilité proposent une intégration avec les outils OpenTelemetry.

Le niveau d'intégration varie d'un fournisseur à l'autre, certains offrant uniquement des formats d'échange de données pour prendre en charge les normes OpenTelemetry, tandis que d'autres assurent une intégration Open Source/OpenTelemetry complète. L'adoption complète des normes OpenTelemetry peut apporter des avantages significatifs en matière d'instrumentation. En effet, les clients peuvent déployer une instrumentation prête à l'emploi quelle que soit la plate-forme utilisée. Le concept de portabilité devient également accessible, ce qui réduit les coûts et améliore l'efficacité. Avec la fusion d'OpenCensus et d'OpenTracing, et l'intégration plus étendue du traçage Jaeger, la partie la plus complexe de l'observabilité, le traçage, semble doucement se mettre en place.

Tableau 1 – Positionnement des fournisseurs

	MODÈLE DE DÉPLOIEMENT			INSTRUMENTATION/OUVERTURE	
	Sur site	SaaS privé	SaaS public	Télémétrie ouverte	Instrumentation
AppDynamics	++	-	++	+	+
Datadog	-	-	++	+	+
Dynatrace	++	-	++	++	+++
Elastic	++	-	++	+++	++
Epsagon	-	-	++	++	+
IBM	+	+	-	-	-
Logz.io	-	-	++	++	++
Micro Focus	-	-	++	-	+
New Relic	-	-	++	++	++
Splunk	-	-	++	+++	++
StackState	++	++	-	+	+
Sumo Logic	-	-	++	+	+
VMware	-	-	++	++	++
Zebrium	++	-	++	+	+

+++ : priorité principale et adaptation parfaite de la solution
++ : solution adéquate dans ce domaine, mais améliorations requises
+ : utilisation limitée de la solution
- : non applicable ou absent

Source : GigaOm 2021

3. Comparaison des critères clés

En s'appuyant sur les conclusions du rapport GigaOm, « Key Criteria for Evaluating Cloud Observability » (Rapport sur les critères clés de l'observabilité cloud), le **tableau 2** montre comment chaque fournisseur inclus dans cette étude se positionne dans les domaines que nous considérons comme stratégiques dans ce secteur. L'objectif est de présenter au lecteur un aperçu des fonctionnalités techniques des différentes solutions et d'établir le périmètre du marché.

L'observabilité et la résilience sont des problématiques IT majeures depuis des décennies. Cependant, l'émergence des bonnes pratiques de Google SRE en matière de conception de systèmes résilients a permis de mettre ces concepts au premier plan. Avec l'introduction des objectifs de niveau de service (SLO ou Service Level Objectives), se pose aujourd'hui la question de savoir s'il est plus judicieux de résoudre la dette technique ou de conserver les coûts de maintenance.

Dans le cadre de l'évaluation des fournisseurs, nous avons tenu compte de cette dynamique de dette technique pour différencier les anciennes technologies des nouvelles. Nous avons également accordé une importance particulière aux fournisseurs qui offrent une télémétrie ouverte, une connectivité ouverte, des interfaces ouvertes et une facturation basée sur des modèles de consommation. L'ensemble du marché des logiciels évolue vers des modèles de tarification basés sur la consommation, ce qui peut s'avérer extrêmement bénéfique en matière d'observabilité.

Tableau 2 – Comparaison des critères clés

	CRITÈRES CLÉS							
	Observabilité et visualisation	Observabilité et application	Analyse des modèles	Références/ Anomalies	Sources données analyse des causes profondes	Correction/ Automatisation	Marché des partenaires	Intégration des Opérations
AppDynamics	++	++	++	++	++	-	++	++
Datadog	+++	+++	++	++	++	+	++	++
Dynatrace	++	+++	++	++	++	+	+++	++
Elastic	+++	+++	++	++	+	+	++	++
Epsagon	+++	+	+++	++	+	-	++	+
IBM	+	+	-	+	+	++	+	+
Logz.io	+++	++	++	++	++	-	++	+
Micro Focus	++	++	++	+	++	+++	++	+
New Relic	+++	+++	-	++	+	-	+++	++
Splunk	+++	+++	++	++	++	++	+++	++
StackState	+++	+	++	++	+++	-	+	+
Sumo Logic	+++	++	++	++	++	-	++	++
VMware	+++	+++	++	++	++	+	++	++
Zebrium	++	++	++	++	-	-	+	-

+++ : priorité principale et adaptation parfaite de la solution
++ : solution adéquate dans ce domaine, mais améliorations requises
+ : utilisation limitée de la solution
- : non applicable ou absent

Source : GigaOm 2021

Tableau 3 – Comparaison des métriques d'évaluation

	MÉTRIQUES D'ÉVALUATION							
	Performances	Sécurité	Délai de rentabilisation	Exhaustivité	Évolutivité et adaptabilité	Systèmes et architectures	Étendue de la télémétrie	TCO, coûts, modèles utilisation
AppDynamics	++	++	+	++	+++	++	++	+
Datadog	+++	++	++	++	+++	++	++	+
Dynatrace	+++	++	++	++	+++	+++	++	++
Elastic	+++	++	++	++	+++	++	+++	+++
Epsagon	+++	++	++	++	+++	++	++	+++
IBM	+	+	++	+	+	+	+	+
Logz.io	+++	++	+++	++	+++	++	++	+++
Micro Focus	++	++	+	+	++	+	+	+
New Relic	+++	++	+++	++	+++	++	++	++
Splunk	+++	++	+	+++	+++	+++	++	+
StackState	++	+	+	+	+	+	+	+
Sumo Logic	+++	++	++	++	+++	++	+	++
VMware	+++	++	+	++	+++	++	++	++
Zebrium	+	+	+++	+	++	+	+	++

+++ : priorité principale et adaptation parfaite de la solution
++ : solution adéquate dans ce domaine, mais améliorations requises
+ : utilisation limitée de la solution
- : non applicable ou absent

Source : GigaOm 2021

Grâce aux informations fournies dans les tableaux ci-dessus, le lecteur a une vision plus claire des solutions techniques actuellement disponibles sur le marché.

4. Rapport GigaOm

Ce rapport résume l'analyse des critères clés et leur impact sur les métriques d'évaluation ; ces informations sont ensuite utilisées pour illustrer le graphique du rapport GigaOm **(Figure 1**). Le graphique qui en résulte fournit une approche prospective de tous les fournisseurs étudiés dans ce rapport, basée sur les capacités techniques et les ensembles de fonctionnalités propres à leurs produits.

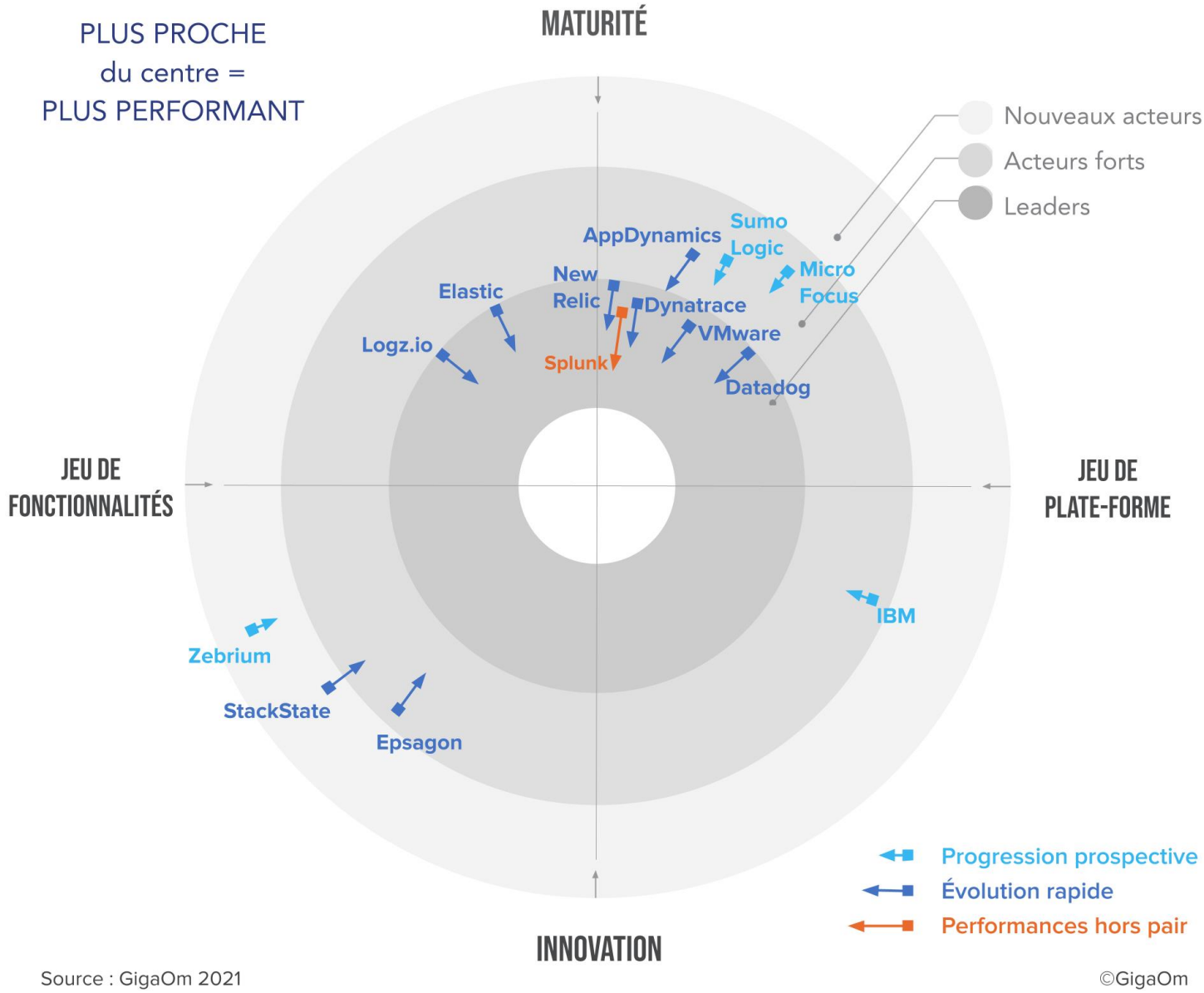

Figure 1 – Rapport GigaOm sur l'observabilité cloud

Le rapport GigaOm place les solutions des fournisseurs sur une série d'anneaux concentriques où celles plus proches du centre sont considérées comme ayant une valeur globale plus élevée. Le graphique évalue chaque fournisseur sur deux axes : la maturité par rapport à l'innovation d'une part, et le jeu de fonctionnalités par rapport au jeu de plate-forme d'autre part, avec une flèche qui projette l'évolution de chaque solution au cours des 12 à 18 prochains mois.

Comme vous pouvez le voir dans le graphique du rapport (**Figure 1**), aucun acteur dominant n'est identifié dans ce rapport. Au contraire, un certain nombre d'entreprises se positionnent comme leaders à mesure qu'elles étoffent leur offre par le biais d'acquisitions, de développement interne et de partenariats. Les fournisseurs de services APM (Application Performance Monitoring ou surveillance des performances des applications) ont fait des progrès en ajoutant des fonctionnalités de mesure au niveau des journaux et de l'infrastructure, tandis que les fournisseurs de journaux prennent de plus en plus en charge les fonctionnalités de métriques et de traçage.

Il est encourageant de constater que les fournisseurs étendent leurs capacités pour adopter des approches basées sur le cloud. Bien que les fournisseurs traditionnels puissent avoir des difficultés à mettre en place les technologies cloud natives, ils conservent leur valeur en fournissant des fonctionnalités, une intégration et une robustesse de niveau professionnel. Une chose est sûre : aucun fournisseur ne dispose d'une solution miracle et universelle pour répondre aux exigences d'observabilité. Toutefois, une combinaison de solutions ou une solution de fournisseur enrichie d'outils Open Source peut vous aider à vous rapprocher de cet objectif. Cela est particulièrement vrai pour les entreprises exploitant AWS qui ont la possibilité de s'engager dans des solutions innovantes reposant sur AWS pour proposer une approche concentrée et rentable.

Notre analyse montre que les entreprises doivent établir leurs priorités en termes de cas d'utilisation, de choix d'emplacement, de fonctionnalités, et enfin de coût pour identifier le fournisseur et la solution qui leur conviennent le mieux. Les décisionnaires doivent être attentifs aux changements du marché. Les fusions et acquisitions sont en pleine effervescence dans le domaine de l'observabilité, ce qui engendre une certaine volatilité. Par exemple, nous avons pu prendre en compte la fusion Splunk/SignalFx, mais l'acquisition d'Instana par IBM a eu lieu après notre échange avec le fournisseur. Nous nous sommes efforcés de faire un état des lieux du marché de l'observabilité tel qu'il existe aujourd'hui tout en tenant compte de l'impact à long terme des feuilles de route des fournisseurs.

Il est également important de noter que la plupart des fournisseurs ont tendance à exceller dans certains domaines et à être en retard dans d'autres. Pour identifier un fournisseur comme leader dans ce rapport, nous avons pris en compte la cohérence des journaux, métriques et traces sur l'ensemble de la pile, à la fois dans le cloud et sur site, tout en privilégiant la prise en charge de la télémétrie ouverte, ainsi que la simplicité et la rentabilité de l'instrumentation. Il s'agit d'un ensemble complexe de fonctionnalités que les fournisseurs doivent mettre en œuvre.

AU CŒUR DU RAPPORT GIGAOM

Le rapport GigaOm évalue l'exécution, la feuille de route et la capacité d'innovation de chaque fournisseur pour positionner les solutions sur deux axes, chacun étant constitué de paires opposées. Sur l'axe Y, la **maturité** reconnaît la stabilité de la solution, la puissance de l'écosystème et une position conservatrice, tandis que l'**innovation** met l'accent sur l'innovation technique et une approche plus agressive. Sur l'axe X, le **jeu de fonctionnalités** met l'accent sur les fonctionnalités de niche ou de pointe, tandis que le **jeu de plate-forme** affiche une orientation plus large de la plate-forme et un engagement envers un ensemble complet de fonctionnalités.

Plus une solution est proche du centre, plus son exécution et sa valeur sont optimales, les acteurs les plus performants se retrouvant dans le cercle interne des leaders. Le cercle le plus au centre est presque toujours vide. Il est réservé aux marchés consolidés parvenus à maturité qui manquent d'espace pour gérer de nouvelles innovations.

Le rapport GigaOm offre une évaluation prospective en indiquant la position actuelle et prévue de chaque solution sur une période de 12 à 18 mois. Les flèches représentent les évolutions en fonction de la stratégie et de la vitesse d'innovation, classant les fournisseurs dans trois catégories (« progression prospective », « évolution rapide » et « performance hors pair ») en fonction de leur taux de progression.

Notez que le rapport ne tient pas compte des parts de marché de chaque fournisseur. L'accent est mis sur une analyse prospective qui privilégie la valeur de l'innovation et la différenciation par rapport à la position actuelle sur le marché.

5. Informations sur les fournisseurs

Cisco AppDynamics

Cisco a rejoint le marché de l'observabilité avec l'acquisition d'AppDynamics et de ThousandEyes. La solution AppDynamics s'adresse aux moyennes et grandes entreprises, et attire les clients des secteurs financier, du commerce de détail et des services informatiques. L'entreprise a transformé la solution APM AppDynamics en une plate-forme d'observabilité, en y ajoutant des fonctionnalités telles que la surveillance du cloud, du réseau et de l'infrastructure. La solution permet de visualiser les modèles de revenus et de mettre en corrélation l'expérience client et l'expérience des applications afin de détecter et de résoudre les problèmes liés aux applications. Elle peut également surveiller les erreurs à l'aide de son moteur de cognition, isoler les domaines problématiques et identifier les causes premières à partir des données d'instantané en analysant toutes les instances de télémétrie collectées dans l'arborescence des dépendances à l'aide de la fonction Automated Transaction Diagnostic.

La fonction APM offre une visibilité jusqu'au niveau du code, ainsi que sur les transactions importantes dans les environnements multicloud. L'outil de surveillance de l'infrastructure fournit aux utilisateurs une vue des connexions entre les applications et l'infrastructure, qu'il s'agisse d'un environnement cloud hybride, multicloud ou sur site.

Cisco AppDynamics peut ingérer des données à partir de ses propres agents, ainsi que via des normes ouvertes telles que Prometheus et OpenTelemetry. La solution prend également en charge les clouds publics tels qu'AWS, consomme jusqu'à 450 milliards de métriques par jour et peut gérer des données structurées et non structurées. Ses systèmes n'utilisent pas l'échantillonnage.

À l'instar des autres fournisseurs APM, la plate-forme utilise une topologie et un modèle de données basé sur les dépendances qui couvrent les différents domaines. Elle peut établir une base de référence pour toutes les métriques collectées ou calculées afin d'identifier le comportement normal. L'intelligence artificielle (IA) détecte automatiquement les anomalies et les supprime du calcul de référence pour réduire les faux positifs, normalise les données de référence pour une qualité accrue et identifie la saisonnalité en fonction des données historiques afin de réduire les interventions manuelles.

La solution Cisco AppDynamics est dotée d'une intégration bidirectionnelle avec ServiceNow, qui permet de mapper les éléments de configuration CMDB sur les entités AppDynamics. Cela permet de visualiser l'état de l'application et de l'infrastructure sous-jacente dans ServiceNow, ainsi que de faciliter une navigation rapide et contextuelle entre les plates-formes pour accélérer le dépannage.

Cisco AppDynamics fonctionne également avec Cisco Intersight Workload Optimizer et des plates-formes CI/CD (intégration continue/livraison continue) comme Harness.io, et dispose de nombreuses API, permettant ainsi aux clients d'intégrer de nombreux autres outils et plates-formes.

AppDynamics convient particulièrement aux moyennes et grandes entreprises capables d'exploiter ses fonctionnalités et son moteur d'IA. La solution est disponible en tant que solution SaaS/mutualisée, mais peut également être configurée sur site.
Actuellement, le prix est fixé par agent, ce qui pourrait s'avérer coûteux pour les opérations à grande échelle. Cisco travaille d'ailleurs sur un nouveau modèle de tarification.

Cisco a ajouté des fonctionnalités à cette solution APM d'entreprise traditionnelle afin d'assurer l'observabilité des applications modernes. Bien que l'intelligence artificielle (IA) et le machine learning (ML) soient intégrés à la plate-forme, les cas d'utilisation associés à l'AIOps restent limités. Si la solution offre une suite intéressante de fonctionnalités de visibilité pour les applications AWS, ce n'est pas réellement le cas pour Azure et GCP. L'entreprise doit également étendre, entre autres, l'intégration de la norme OpenTelemetry et des collecteurs Open Source.

Points forts : Cisco a fait l'acquisition de ThousandEyes, ce qui ajoute une surveillance synthétique pour les environnements Internet et cloud tout en améliorant la surveillance de l'expérience numérique AppDynamics. L'expérience visuelle du tableau de bord offre un aperçu des interruptions de service jusqu'au niveau de l'application, ainsi qu'un aperçu des coûts transactionnels affectés. La création d'instantanés de transaction permet aux développeurs d'effectuer une inspection approfondie du code des appels d'API.

Défis : compte tenu de la prédominance de Cisco sur le marché des réseaux, il est surprenant que la solution AppDynamics n'accepte pas et ne met pas en corrélation davantage de données réseau. Certains domaines pourraient être améliorés, à savoir la gestion des agents, l'intégration des métriques dans Azure, GCP et d'autres fournisseurs cloud, ainsi que la gestion des journaux (bien que l'acquisition de dashbase.io devrait permettre d'améliorer ce point).

Datadog

Datadog a été créé en 2010 dans le but d'éliminer les conflits entre les développeurs et les administrateurs système. Sa croissance est stimulée par l'accent mis sur l'automatisation et l'observabilité en temps réel. Après avoir fait ses premiers pas dans la surveillance des infrastructures, l'entreprise Datadog a élargi son portefeuille via des acquisitions et une innovation interne pour offrir des solutions dans le vaste domaine de l'observabilité.

Datadog surveille les systèmes d'infrastructure à l'aide d'agents et d'appels d'API pour prendre en charge les conteneurs, les machines virtuelles, les services, les bases de données, les systèmes de stockage et les appareils réseau. Si un agent ne peut pas être déployé, la solution peut collecter des informations à distance à l'aide de SNMP, JMX, OpenMetrics ou d'appels d'API distants.

L'agent Datadog s'exécute dans les clusters Kubernetes des clients pour collecter des métriques, des traces et des journaux en temps réel. L'agent peut se trouver directement sur le système d'exploitation, comme déploiement conteneurisé, déploiement side-car ou déploiement sans agent utilisant une couche Lambda dans des environnements sans serveur.

L'outil de surveillance du réseau cloud natif compte les paquets entre les points de terminaison IP/port source et de destination. Grâce au balisage, les clients suivent les dépendances et les métriques (telles que le volume des requêtes), les écarts de temps aller-retour entre les composants persistants (tels que les services ou les applications) et les composants de courte durée (tels que les pods Kubernetes).

La plate-forme offre plus de 400 intégrations, telles que AWS Fargate et Lambda, Google Cloud Run et Functions, Azure Functions et Azure App Service pour les environnements sans serveur. Elle propose également des orchestrateurs tels que Kubernetes, OpenShift, Amazon ECS et AWS Fargate, Rancher, Mesos, Docker Swarm, Cloud Foundry et Azure Container Instances.

La plate-forme Datadog dispose d'une structure de balisage dynamique, unifiée et commune, lui permettant de trianguler et de prendre en charge l'analyse de la cause première, l'unification et la télémétrie sur l'ensemble de la pile et de la plate-forme.

La stratégie de gestion des journaux de Datadog repose sur la fonction Logging Without Limits™, qui offre aux clients une flexibilité et un meilleur contrôle des coûts via la hiérarchisation des journaux. La surveillance APM et le traçage distribué sont effectués via la fonction Tracing Without Limits™. Cela garantit un meilleur équilibre entre coût et visibilité en permettant aux clients d'envoyer la totalité de leurs traces, de les rechercher et de les analyser dans une fenêtre glissante en temps réel de 15 minutes, puis d'indexer les plus importantes.

La plate-forme conserve automatiquement les traces d'erreurs et de latence élevée pendant 15 jours. Les traces peuvent être recherchées et analysées à l'aide de balises et d'attributs. Elles sont représentées par le graphique de type « flamme » Datadog qui visualise le chemin d'exécution de la requête. La suite de surveillance des applications Datadog inclut également Real User Monitoring (RUM) et Synthetics pour une visibilité en amont.

Datadog propose plusieurs modèles de tarification pour les solutions au sein de sa plate-forme d'observabilité, que ce soit pour la surveillance de l'infrastructure, la gestion des journaux, la surveillance APM ou la surveillance de la sécurité. La configuration de Datadog s'applique à ses solutions basées sur des agents. La solution peut être déployée en tant que solution SaaS mutualisée. Aucune version sur site n'est proposée.

Datadog a considérablement renforcé son système de surveillance de l'infrastructure basée sur l'hôte. D'autres avantages significatifs sont proposés, à savoir l'ajout d'informations relatives à l'application, le traçage des applications/transactions, les journaux de traces associées, le profilage de code, la surveillance réelle des utilisateurs/de l'expérience, la surveillance du réseau et la surveillance de la conformité. Toutefois, la solution doit se développer davantage et étendre ses fonctionnalités pour devenir une solution d'observabilité d'entreprise complète et de premier ordre.

Points forts : la collecte et le stockage de données ultraprécises (jusqu'à un intervalle d'une seconde) améliorent l'analyse des données. L'intégration complète d'AWS et la prise en charge adéquate des environnements de cloud privé et sur site en font la solution idéale pour les équipes hybrides. La présence d'un seul agent pour collecter toutes les données de télémétrie élimine la nécessité de déployer un nouvel agent chaque fois que de nouvelles données doivent être collectées.

Défis : la solution doit être améliorée et développée, en particulier en matière de traçage et de surveillance des applications. En outre, des préoccupations subsistent concernant la gestion limitée des journaux et la recherche au niveau des événements, tout comme la prise en charge insuffisante des besoins en données non structurées. Les prix restent relativement élevés.

Dynatrace

Dynatrace s'est forgé une solide réputation en tant que solution APM (surveillance des performances des applications) de haute qualité. Cette solution s'appuie maintenant sur cette réputation grâce à sa plate-forme d'observabilité complète, basée sur Davis, le moteur d'IA exclusif de l'entreprise.

La plate-forme Dynatrace inclut la surveillance APM, l'AIOps, la surveillance de l'infrastructure, l'analyse métier numérique et la gestion de l'expérience numérique pour les services informatiques d'entreprise et les entreprises numériques. En alliant l'automatisation au moteur d'IA Davis, la plate-forme Dynatrace fournit des détails sur les causes premières des performances des applications, génère des informations sur l'infrastructure sous-jacente et présente une vue d'ensemble de l'expérience utilisateur. Le système est conçu pour évoluer et fonctionner sur site ou dans des environnements hybrides, cloud ou périphériques.

L'instance OneAgent de la plate-forme dépose un seul fichier binaire sur un hôte pour instrumenter automatiquement non seulement les conteneurs exécutés dans l'environnement, mais également les processus exécutés dans le conteneur, sans nécessiter d'instrumentation manuelle ou de modification d'image.

Les modèles IA/ML auto-adaptatifs déclenchent 90 % de tous les problèmes détectés et analysés, ainsi que leur processus d'identification de causes premières basée sur des graphiques. Davis peut évaluer la gravité d'un problème en fonction de l'impact sur l'utilisateur, de la valeur transactionnelle, de la perte de productivité et d'autres facteurs.

Dynatrace prend en charge le traçage de bout en bout pour toutes les technologies de file d'attente basées sur JMS. Cette solution prend également en charge IBM MQ, Apache Kafka, RabbitMQ, ActiveMQ, MSMQ, Tibco EMS et Tibco Rendezvous.

La solution Dynatrace convient particulièrement aux moyennes et grandes entreprises qui ont besoin d'automatiser les processus d'observabilité. Elle est disponible en tant que solution SaaS complète ou solution SaaS distribuée. La version SaaS distribuée nécessite un cluster privé, qui peut se trouver sur site ou dans un cloud public ou privé. La plate-forme SaaS complète reçoit des mises à jour toutes les deux semaines, la version distribuée tous les mois.

Le cluster Dynatrace est généralement configuré sur un seul nœud et peut être étendu à plusieurs nœuds selon les besoins. Des fonctions de haute disponibilité et d'équilibrage de charge sont intégrées. La solution crée automatiquement un nom DNS et un certificat pour une expérience sécurisée prête à l'emploi.

En tant qu'entreprise pionnière dans l'espace APM, Dynatrace a remanié sa solution il y a quelques années et est depuis devenu un acteur important dans le secteur de l'observabilité. L'intégration à plus de 500 solutions prêtes à l'emploi facilite les connexions au sein de l'espace ITOps. La collecte complète des données (sans échantillonnage) constitue un autre avantage. Cependant, cette fonction peut produire un volume élevé de métriques et de données de traçage qui peuvent submerger les systèmes existants.

Dynatrace prend en charge OpenTelemetry et représente l'un de ses cinq principaux contributeurs. Bien que Dynatrace ne soit pas une solution de journalisation en soi, elle s'intègre bien aux principaux fournisseurs de journaux. Le mappage de la topologie du système central vers le microservice, ainsi que les tableaux de bord identifiant l'impact sur l'entreprise renforcent la solution.

Points forts : l'utilisation d'un seul agent pour instrumenter un environnement constitue un concept intéressant. Il existe actuellement une intégration complète de télémétrie ouverte native pour les métriques qui sera bientôt disponible pour les traces. La fonction du tableau de bord est très pratique et démontre l'impact sur l'entreprise, les applications et les utilisateurs tout en rejouant les transactions en temps réel.

Défis : la solution est basée sur des nœuds. Elle n'est pas conçue sur Kubernetes ou un autre conteneur, mais peut être exécutée en mode natif dans le cloud. Elle n'offre pas d'intégration aux autres acteurs importants d'AIOps pur, ce qui pourrait être utile pour de nombreux clients.

Elastic

Elastic a créé une plate-forme d'observabilité solide en utilisant la pile gratuite et ouverte ELK (Elasticsearch, Logstash, Kibana). L'entreprise a réussi à intégrer la convivialité et la visibilité à la pile. Sa technologie est utilisée à grande échelle par des entreprises aussi diverses qu'eBay, Wikipédia, Uber et Netflix.

Elastic propose des versions d'entreprise et cloud (AWS, Azure et GCP). Cela permet aux utilisateurs de créer des variantes indépendantes de cloud hybride ou multicloud de la solution en fonction de leurs besoins. Cet aspect est particulièrement utile lorsqu'une entreprise doit démarrer sur un emplacement (sur site ou dans le cloud) et s'étendre rapidement à d'autres emplacements sans créer de mises en œuvre cloisonnées ou fragmenter l'ensemble d'outils.

La solution Elastic Observability utilise ses propres produits d'ingestion Open Source populaires, Logstash et Beats, pour la collecte et la transmission de données. Les agents de transfert de données légers, « Beats », collectent et expédient des données à partir de l'emplacement en périphérie. Logstash est un pipeline de traitement de données côté serveur qui prend en charge plusieurs sources et récepteurs. Une combinaison solide est ainsi proposée pour la recherche, l'observabilité combinée, la sécurité des points de terminaison, et la gestion des informations et des événements de sécurité (SIEM, Security Information and Event Management).

La solution offre une visibilité sur l'ensemble de l'écosystème à l'aide de la fonction sous-jacente Elasticsearch permettant de rechercher rapidement des informations pertinentes dans toutes les données. La solution combine les journaux, les métriques, les enregistrements synthétiques et les traces dans le magasin de données Elasticsearch. Elle utilise également Kibana pour obtenir des résultats rapides, réduisant ainsi le délai moyen de résolution et améliorant la collaboration de type « cellule de crise ».

Elastic Observability vise à créer une ressource de connaissances centralisée, ce qui facilite la visualisation et l'étude de tous les aspects d'une infrastructure complexe. La solution prend en charge des normes ouvertes et des agents tels qu'OpenTelemetry et Jaeger, ainsi que des API pour accroître la portabilité.

Elastic utilise le schéma ECS (Elastic Common Schema) pour normaliser les données et rendre les fonctions de recherche, d'analyse, de détection d'erreurs et d'alerte plus rapides et plus simples. Kibana fournit des visualisations claires pour faciliter l'analyse. Le machine learning garantit des alertes claires et offre des opportunités d'automatisation.

Le modèle de machine learning non supervisé d'Elastic utilise une base de référence des systèmes observés et identifie les anomalies comportementales. Les utilisateurs peuvent contrôler la fréquence des références en fonction de leurs besoins (par service, par hôte, par environnement, etc.), mais le paramètre par défaut est légèrement inférieur à 10 minutes.

Elastic Observability permet d'automatiser la correction avec les fournisseurs d'automatisation de flux de travail ITSM et DevOps les plus courants (comme ServiceNow). La solution utilise également la correction manuelle assistée par analyste (via PagerDuty, Slack et Jira), les webhooks d'alerte pour les intégrations de correction générique (y compris l'utilisation de scripts personnalisés) et l'intégration au niveau de l'API des approches de remédiation automatisée les plus personnalisées.

La popularité d'Elastic Stack repose en grande partie sur sa capacité à évoluer sans affecter les performances grâce à l'architecture à évolutivité horizontale de chaque couche. La solution Elastic Observability conserve cette force. Elle peut évoluer à la hausse ou à la baisse sans interruption de service.

La surveillance du réseau fait également partie de la solution. Bien qu'elle ne soit pas aussi complète ou détaillée que les outils NPMD (surveillance et diagnostic des performances réseau) du fournisseur de réseau, cette surveillance peut ajouter une fonction utile à l'approche DevSecOps et à l'observabilité globale.

Elastic Observability convient particulièrement aux moyennes et grandes entreprises disposant des ressources nécessaires pour tirer le meilleur parti de ses fonctionnalités et gérer sa complexité. Les entreprises peuvent déployer Elastic Observability en tant que composant SaaS sur un cloud public, en tant que solution autogérée sur un cloud public ou privé, ou sur site. La solution offre une version gratuite avec une fonctionnalité de diagnostic complète, mais les fonctions utiles et l'assistance nécessitent la version complète.

Elastic propose une solution robuste et ouverte d'observabilité complète basée sur la télémétrie qui aide les entreprises à observer l'ensemble de la pile (y compris la surveillance APM, l'infrastructure, les services et le réseau) à la fois des solutions d'entreprise et des solutions basées sur le cloud. La solution offre même une visibilité sur les options combinées multicloud et cloud hybride dans une pile. Bien que les fonctionnalités de journalisation et de métriques soient de premier ordre, Elastic devrait envisager d'étendre sa surveillance RUM (Real User Monitoring), sa surveillance de l'expérience utilisateur et sa surveillance des applications mobiles natives pour en faire une solution complète.

En proposant une solution gratuite et ouverte, Elastic s'impose comme l'un des meilleurs choix pour les clients soucieux de leurs coûts. Grâce à la télémétrie ouverte, les clients peuvent se développer et s'intégrer à une suite de solutions provenant de la Cloud Native Computing Foundation.

Bien qu'Elastic soit une solution robuste, nous souhaiterions voir une intégration plus native aux principales plates-formes AIOps afin de combiner l'observabilité complète de la pile avec l'AIOps. Nous aimerions également voir des améliorations au niveau des alertes, de la gestion des incidents, de l'intégration aux outils ITSM/DevOps et de la création de rapports pour qu'Elastic devienne un partenaire de premier ordre.

Points forts : grâce à ses différentes variantes d'exécution sur site et dans le cloud, Elastic est un excellent choix pour les entreprises envisageant des déploiements multicloud ou cloud hybride. Un autre avantage indéniable de cette solution repose sur le concept consistant à placer les données à côté de l'application et à effectuer des recherches fédérées entre les clusters et les clouds. Cette solution engendre un faible coût d'acquisition.

Défis : la collecte des journaux Logstash/Beats est efficace, mais une intégration plus étroite à FluentBit pour Kubernetes pourrait être utile. Elastic prend en charge la collecte de journaux Docker via Beats, mais l'absence d'un plug-in Logstash natif crée davantage de travail pour les développeurs. La mise à niveau de l'intégration à Prometheus constituerait une amélioration pour les solutions cloud natives. Certains clients ont également signalé des problèmes avec les métriques basées sur Kibana.

Epsagon

Service cloud natif, Epsagon utilise les fonctions IA/ML dans sa solution. Fondé en 2017, le service Epsagon relativement nouveau est intégré à AWS et au service AWS Lambda, ce qui en fait un excellent choix pour les organisations alignées sur les fonctions sans serveur AWS.

Epsagon a pour intention de simplifier le développement et le dépannage grâce à son architecture légère et à son instrumentation automatique. La plate-forme utilise un tableau de bord principal pour offrir aux utilisateurs une visibilité optimale sur des architectures d'entreprise complexes. Grâce à ce portail, les algorithmes IA/ML alertent rapidement les utilisateurs des problèmes, réduisant ainsi le délai moyen de résolution.

En utilisant des variantes de PostgreSQL, MySQL et Elasticsearch en arrière-plan, Epsagon regroupe, unifie, analyse et met en corrélation les données de plusieurs outils tiers. Cette solution vise à fournir une vue centralisée afin de faciliter la visibilité sur les conteneurs, les microservices, Kubernetes, Apache OpenWhisk, les architectures sans serveur et d'autres composants d'infrastructure. Elle s'intègre aux systèmes de gestion des tickets tels que Jira, GitHub, Clubhouse, ServiceNow, ainsi qu'aux webhooks.

Epsagon Service Maps affiche automatiquement toutes les dépendances entre les applications et l'infrastructure pour vous aider à visualiser les métriques de performances dans des tableaux de bord personnalisés. Les entreprises peuvent utiliser ces tableaux de bord pour surveiller une application ou pour dépanner des zones spécifiques de cette application.

La plate-forme peut également permettre de visualiser les références des applications et fournir une visibilité ou générer des alertes basées sur des seuils de métriques à différents intervalles d'indice de confiance. Elle dispose de fonctions d'autoréparation grâce à l'analyse des données d'alerte et de charge utile. Ses collecteurs de traces analysent et mettent en forme automatiquement les données de trace, de charge utile et de métriques. Les traces sont automatiquement collectées en fonction de l'instrumentation automatique de l'agent Epsagon jusqu'au niveau de la structure au sein d'un service. Le déploiement chronophage d'agent devient inutile.

La feuille de route de la plate-forme inclut des événements d'infrastructure dans le contexte des traces et des métriques, des métriques personnalisées, des données RUM (Real User Monitoring) et de la prise en charge d'agents de langage supplémentaires. Cette solution est particulièrement adaptée pour les petites entreprises cherchant à accroître leur observabilité dans un projet. Son modèle de tarification rend l'évolutivité potentiellement coûteuse, mais ses outils et ses automatisations peuvent aider les équipes opérationnelles de plus petite taille à réduire leur délai moyen de résolution et à améliorer la rentabilité de leurs projets en cours.

Bien que nouveau venu dans le secteur, Epsagon a conçu une solution d'observabilité de qualité. Reposant principalement sur les applications cloud natives AWS, cette solution s'intègre de manière étroite à AWS via des fonctions sans serveur qui fournissent un traçage complet au niveau des applications, une surveillance de l'infrastructure et des métriques. Epsagon doit améliorer ses fonctionnalités pour axer davantage sa solution sur les entreprises et la production, y compris l'intégration aux outils d'entreprise, aux outils de conformité, de sécurité et de gouvernance. Le service proposé par Epsagon est intéressant pour les solutions cloud natives AWS.

Points forts : l'instrumentation et les collecteurs de données d'Epsagon sont légers, faciles et rapides à déployer. La solution effectue une collecte et une analyse de données avec une fidélité optimale, et non un échantillonnage comme d'autres fournisseurs. Elle offre également une visibilité de bout en bout des applications aux microservices, en particulier pour les services AWS, et dispose d'une fonction temporelle pour vérifier l'état antérieur d'une application/d'un service.

Défis : cette solution manque de nombreuses fonctionnalités d'entreprise, ce qui peut rendre son adoption difficile par les grandes entreprises. Epsagon gagnerait à ajouter la résolution des incidents, l'interaction d'automatisation/de correction et des fonctionnalités pour prendre en charge les applications d'autoréparation.

IBM

L'entreprise IBM a adopté une stratégie de cloud qui, selon elle, fera d'elle un leader dans l'espace de cloud hybride. En faisant l'acquisition de Red Hat, IBM a simultanément intégré OpenShift, ce qui a rendu sa plate-forme de gestion multicloud compétitive. La plate-forme d'observabilité combinée à Watson pour AIOps est déjà un bon début. La première itération de la solution a été commercialisée en 2019 et IBM continue de progresser. (*Remarque : nous avons évalué la solution avant l'acquisition d'Instana par IBM, un autre fournisseur dans ce domaine. Cette évaluation ne tient donc pas compte des fonctionnalités d'Instana.*)

La solution s'exécute sur Red Hat OpenShift et utilise une plate-forme de gestion de cloud hybride ouverte pour assurer la gestion du cycle de vie des clusters, la gestion du cycle de vie des applications, la gestion des performances des applications pour les applications traditionnelles et cloud natives, la gestion des événements et de l'infrastructure, ainsi que la gouvernance et la gestion des risques.

Cloud Pak utilise des bases de données de séries temporelles SQL et NoSQL de pointe. Le système est configuré en tant que magasin centralisé, mais assure un traitement en périphérie et sur serveur. Bien qu'elle soit encore en cours de développement, la feuille de route inclut l'AIOps basé sur la célèbre plate-forme Watson d'IBM.

La solution repose sur Thanos et Grafana, deux composants utilisés à grande échelle. Bien qu'IBM affirme que la solution est conçue à la fois pour les applications d'ancienne génération et les applications modernes hybrides et cloud natives, elle est bien plus performante dans les environnements existants sur site que dans les environnements cloud natifs.

Cloud Pak for Multicloud Management utilise des webhooks pour avertir le système des événements. Le système actif utilise la solution IBM Dashboarding et les connecteurs PromQL comme Grafana pour l'affichage. La plate-forme inclut des informations prédictives pour la définition de références et la détection des anomalies, et offre un inventaire topologique pour capturer automatiquement toutes les modifications de configuration.

La feuille de route du développement comprend l'intégration des points de terminaison Prometheus et OpenTracing, ainsi que de nouvelles fonctionnalités d'IA via l'AIOps Watson propre à IBM pour la résolution des incidents. L'IA devrait ajouter des fonctionnalités nouvelles et améliorées en matière de gestion des coûts et des ressources, de gouvernance, risques et conformité, ainsi qu'au niveau des opérations applicatives.

Il est encourageant de voir la mise en œuvre de certaines fonctions d'entreprise, car elles ont été négligées par de nombreuses solutions. Le déploiement et la gouvernance des clusters basés sur des stratégies, les métriques de rétrofacturation pour les équipes DevOps, le routage automatique des incidents pour les équipes DevSecOps, les puissantes fonctionnalités d'observabilité pour les applications et les composants middleware existants et sur site sont autant de fonctionnalités attrayantes pour une utilisation en entreprise.

Les fonctionnalités d'ingestion de données restent bonnes, mais sont en retard par rapport à celles fournies par les acteurs à la pointe du marché.

La plate-forme nécessite le déploiement de Red Hat OpenShift, ce qui peut poser problème à certaines entreprises, bien que la licence soit incluse. La solution est proposée sur site ou en tant que programme géré par IBM.

Cela pourrait poser problème aux entreprises qui souhaitent passer entièrement en mode cloud natif, disposer d'un contrôle total sur les services et les colocaliser dans leur environnement cloud. Bien que les métriques et la collecte de données pour le traçage soient convenables, la journalisation semble prendre du retard. Ces éléments semblent faibles pour les applications cloud natives. La prise en charge d'OpenTelemetry et d'OpenTracing dans la feuille de route pourrait résoudre certains de ces problèmes.

Dans l'ensemble, il s'agit d'un premier pas positif dans la bonne direction pour Big Blue. La solution n'est en place que depuis un an et cela se voit : elle doit se développer dans de nombreux domaines pour pouvoir s'adapter aux environnements d'entreprise hybrides et multicloud. Cependant, IBM a mis au point des fonctionnalités spécifiques à l'entreprise dans le produit, de sorte qu'à mesure qu'il évolue, il devrait bien s'adapter à sa base de clients d'entreprise sur site existante.

Points forts : l'orientation sur l'entreprise inclut la prise en charge des composants middleware, des systèmes de messagerie, des applications et des machines virtuelles d'ancienne génération, ce qui plaira aux entreprises clientes IBM existantes. L'acquisition d'Instana pourrait apporter une visibilité au niveau du pipeline CI/CD, l'automatisation DevOps en boucle fermée et l'ajout de Prometheus et d'OpenTelemetry, même si cela peut prendre du temps.

Défis : IBM Cloud Pak nécessite une base Red Hat OpenShift pour fonctionner, ce qui peut poser problème aux entreprises qui ne souhaitent pas suivre cette voie. La solution est en retard en matière de capacités cloud natives et ne dispose pas d'intégrations OpenTelemetry et OpenTracing complètes, bien qu'elles aient été ajoutées à la feuille de route.

Logz.io

Logz.io est une entreprise basée en Israël, avec une présence importante aux États-Unis. Elle utilise principalement des technologies Open Source et des normes ouvertes (comme OpenTelemetry) pour surveiller, enregistrer, collecter, rechercher et analyser des données d'observabilité. En fait, une grande majorité de ses revenus provient de sa plate-forme d'observabilité. La solution Logz.io s'adresse en particulier aux clients de cloud natif agiles, dont la plupart exécutent Kubernetes en production. L'entreprise compte plus de 900 clients, dont Siemens, Unity et ZipRecruiter.

La plate-forme Logz.io comporte quatre éléments : la gestion des journaux basée sur ELK, la surveillance de l'infrastructure basée sur Prometheus et Grafana, le traçage distribué basé sur Jaeger et la gestion des informations et des événements de sécurité (SIEM, Security Information and Event Management) basée sur ELK. Il s'agit de services cloud intégrés entièrement gérés qui assurent une surveillance, un dépannage et une protection efficaces des charges de travail cloud distribuées. Bien que la solution de journalisation existe depuis 2014, les composants de traçage et d'infrastructure sont nouveaux (commercialisés en 2020). L'entreprise vient également de commercialiser un système de surveillance synthétique Open Source utilisant FaaS.

Toutes les données (journaux, métriques et traces) sont basées sur des normes ouvertes et utilisent des outils Open Source : FluentD/FluentBit pour Kuberbetes, FileBeat pour les journaux traditionnels, Jaeger pour OpenTracing, et ainsi de suite. Logz.io est une solution mutualisée basée sur le cloud (principalement AWS ou Azure, mais également GCP dans une moindre mesure) qui permet à la plate-forme de mieux fonctionner à grande échelle et à moindre coût. Le stockage de niveau intermédiaire récemment commercialisé permet aux clients de réduire leurs coûts de stockage de 30 % à 40 %. La plate-forme est dotée d'intégrations natives avec AWS, Azure et GCP.

L'accent mis par l'entreprise sur le code Open Source permet de développer des fonctionnalités en plus des technologies bien établies et bien intégrées afin d'aider les clients à se développer et à se démarquer sur le marché. Cette solution vise à faciliter l'utilisation de la plate-forme et élimine le besoin de gérer ou même de comprendre la configuration de l'infrastructure sous-jacente.

La fonction Application Insights de la plate-forme axée sur les fonctions IA/ML permet de regrouper, condenser, dédupliquer et mettre en corrélation les données. La fonction Cognitive Insights utilise une correspondance de modèles au niveau des erreurs. Elle exécute des requêtes via des moteurs de recherche pour trouver des informations et des discussions pertinentes liées à des erreurs similaires et fournit ces informations au client. Cette solution unique ne nécessite qu'une intervention humaine minime après la formation initiale. De plus, elle utilise la fonction puissante Elasticsearch de la pile ELK.

Le niveau de stockage en temps réel de Logz.io fournit à la plate-forme un stockage redondant hautement disponible, tandis que l'option Live Tailing permet aux utilisateurs de visualiser les données dès qu'elles sont ingérées et de les suivre tout au long du flux. La plate-forme est basée sur Kafka pour le flux de données en continu.

Les repères visibles sur les métriques, les journaux et le traçage permettent aux clients d'afficher les incidents tels que le déploiement, la version de build et tout autre élément susceptible d'affecter les systèmes de production. Les clients peuvent ainsi voir les changements potentiels qui pourraient affecter le système et remonter jusqu'à l'événement.

La solution Logz.io convient particulièrement aux entreprises technologiques de petite et moyenne taille à la recherche d'une solution évolutive et flexible qui permet l'intégration sur une large gamme de plates-formes. La solution est disponible avec un modèle de paiement à l'usage, sur une base mensuelle, mais les clients peuvent obtenir l'accès via un accord d'entreprise selon la taille de l'infrastructure. Pour l'instant, cette solution est uniquement disponible en tant que solution SaaS basée sur le cloud.

Logz.io est une solution Open Source très solide, utilisant OpenTelemetry, basée sur le cloud et proposée en tant que SaaS. Bien que la solution de gestion des journaux et les fonctionnalités de recherche soient de premier ordre, le traçage distribué et la surveillance de l'infrastructure viennent d'être commercialisés et doivent se développer avant que les entreprises puissent passer à la production à grande échelle. La surveillance des applications et des services, les métriques pour les applications métiers, la surveillance RUM et les composants de surveillance synthétique (une version Open Source vient d'être publiée) sont absents. La création de telles intégrations à d'autres solutions peut prendre beaucoup de temps.

Points forts : les racines Open Source permettent de réduire les coûts par rapport à certaines solutions propriétaires. La plupart des développeurs cloud utilisent des systèmes Open Source pour faciliter l'intégration des équipes ITOps à leurs processus, au lieu de réinstrumenter les services avec un ensemble d'outils différent en production.

Défis : l'approche Open Source pourrait limiter l'utilisation de solutions comme Fluentbit et FileBeat dans certaines entreprises. La surveillance des applications et des services, les solutions de surveillance RUM et les solutions d'expérience numérique sont limitées ou absentes. Le traçage distribué est nouveau et doit se développer avant d'être utilisé dans les applications courantes.

Micro Focus

Micro Focus est l'un des acteurs de plus longue date établis dans l'espace de surveillance de l'infrastructure et de la gestion des services informatiques (ITSM). Fondée en 1976, l'entreprise a depuis longtemps mis en place son portefeuille technologique, proposant des solutions sur les marchés DevOps, de l'informatique hybride, de la sécurité et de la gestion des risques, et de l'analyse prédictive. Avec l'acquisition récente de plusieurs entreprises (telles que HP Software et Vertica), Micro Focus tente de se faire rapidement une place sur le marché de l'observabilité informatique.

Le produit Operations Bridge surveille et analyse automatiquement l'état et les performances des ressources multicloud et sur site sur tous les types de données, quels que soient les appareils, les systèmes d'exploitation, les bases de données, les applications et les services. La plate-forme offre des moteurs de consolidation et de corrélation des événements, ainsi qu'une réduction du bruit basée sur l'analyse de big data. Elle intègre le contexte de service de bout en bout avec des fonctionnalités de corrélation d'événements basées sur les règles et le machine learning, fournis en plus d'un lac de données, ou data lake.

La plate-forme fournit la surveillance sous forme de code, de sorte que les développeurs peuvent utiliser des API pour envoyer des données à Operations Bridge et configurer la surveillance avec le développement de code. Elle permet une surveillance, une analyse et une correction automatiques des incidents dans l'ensemble de l'infrastructure et des applications. Cela permet de gagner du temps lors de la configuration de la surveillance et de la correction des problèmes. Ses capacités AIOps offrent une mise en corrélation multimode pour une identification accrue des causes premières, améliorant ainsi le délai moyen de résolution.

Operations Bridge utilise la plate-forme Vertica ML de Micro Focus, qui exploite le data lake, ou lac de données, ITOM Collect Once Store Once (COSO) de Vertica pour appliquer des analyses de ML, ainsi que des analyses avancées sur des données provenant de plusieurs sources. Ainsi, de nombreux cas d'utilisation d'opérations informatiques hybrides peuvent être pris en charge. Operations Bridge offre également plusieurs options de tableau de bord personnalisables pour différents utilisateurs et cas d'utilisation. La plate-forme simplifie et accélère l'automatisation des tâches telles que les actions correctives, les notifications et les procédures de récupération.

La plupart des nouvelles fonctionnalités d'observabilité cloud natives viennent d'être commercialisées et doivent se développer avant d'être sérieusement prises en compte par les entreprises numériques.

Cette solution est particulièrement adaptée aux grandes entreprises et aux environnements qui disposent du temps, des personnes et des ressources nécessaires pour tirer le meilleur parti de ses capacités ML et AIOps. Le produit est disponible en tant que déploiement sur site via l'achat d'une licence ou d'un accord de licence d'entreprise (ELA).

Bien que Micro Focus ait travaillé à l'élaboration de son réseau, de son infrastructure informatique et de ses solutions ITSM, l'entreprise doit améliorer ses environnements applicatifs (APM), multicloud et cloud natifs. Pour les utilisateurs existants qui sont encore sur site, Micro Focus fait preuve d'un bon argument, mais il existe des lacunes dans la journalisation, le traçage d'applications, le traçage distribué cloud natif et le domaine CloudOps que l'entreprise doit traiter avant de pouvoir devenir un acteur important du marché de l'observabilité.

Points forts : le tableau de bord à valeur commerciale ajoutée est un outil de visualisation convivial permettant aux responsables non-informatiques d'intégrer les indicateurs de l'entreprise et des réseaux sociaux aux performances des applications. Micro Focus provient de l'automatisation des environnements de centre d'opérations réseau (NOC) et offre des fonctions d'automatisation/de correction pour les systèmes informatiques d'entreprise existants, tels que les redémarrages de systèmes et de réseaux. Cette solution offre également une automatisation prête à l'emploi des anciens modèles de runbook informatique.

Défis : Micro Focus, un acteur important du secteur des réseaux et systèmes, doit s'améliorer de manière significative dans les domaines du cloud et de l'observabilité des applications. L'interface utilisateur Operations Bridge manque de finesse et pourrait utiliser un traitement plus moderne.

New Relic

New Relic est une entreprise basée à San Francisco, fondée en 2008. Sa plate-forme la plus récente, New Relic One, est encore en cours de développement rapide, avec de nombreuses nouvelles fonctionnalités déployées en novembre et décembre 2020. L'entreprise cible principalement les sociétés dans le domaine technologique, en particulier les organisations tournées vers l'avenir à la recherche de solutions innovantes à leurs problèmes. Les revenus de l'entreprise sont en pleine croissance, avec une augmentation de 30 % en 2020 pour atteindre 600 millions de dollars.

New Relic One est une plate-forme d'observabilité basée sur le cloud qui offre une gestion des performances applicatives (APM), ainsi qu'une surveillance au niveau de l'infrastructure, du navigateur, RUM, des produits synthétiques, et une surveillance mobile et cliente native.

La plate-forme offre une observabilité flexible et dynamique des environnements d'infrastructure, des services exécutés dans le cloud ou sur des hôtes dédiés aux conteneurs exécutés dans des environnements orchestrés, y compris les configurations hybrides et multicloud. Grâce à la surveillance de l'infrastructure, les clients peuvent relier les données d'état et de performances de tous les hôtes basés sur le cloud ou sur site au contexte applicatif, aux journaux et aux modifications de configuration.

Les intégrations cloud collectent les données des services et des comptes cloud, sans qu'aucun processus d'installation ne soit nécessaire. Il suffit aux clients de connecter leur compte New Relic à leur compte de fournisseur cloud.

New Relic One offre des intégrations avec Amazon Web Services, Google Cloud Platform et Microsoft Azure. New Relic connecte ces fournisseurs cloud à ses produits Telemetry Data Platform, Full-Stack Observability et Applied Intelligence.

La plate-forme prend en charge les environnements hybrides et les systèmes d'orchestration de conteneurs, notamment Kubernetes, AWS ECS, AWS EKS, AWS Fargate, Azure Container Service, Google Kubernetes Engine, Anthos, PCF, PKS, RedHat OpenShift, Rancher et Docker Swarm.

L'architecture basée sur Kafka est conçue pour évoluer. La solution peut ingérer deux milliards de points de données par seconde et offre un certain degré de latence, car les données reçues peuvent avoir jusqu'à 24 heures. Les clients peuvent envoyer des données à partir de la plate-forme New Relic vers d'autres solutions à des fins de stockage à long terme et d'exploration de données via une API.

La plate-forme New Relic connaît un développement rapide et continu, avec de nouvelles fonctionnalités et intégrations prévues pour début 2021. La tarification a récemment été simplifiée : la solution est passée de onze à trois options, avec une structure de paiement unifiée. New Relic offre désormais une version gratuite permanente, une licence de surveillance complète de la pile qui permet d'accéder à tous les modules selon un modèle de tarification par utilisateur, une plate-forme de données de télémétrie évolutive basée sur l'ingestion mensuelle par Go (0,25 $ par Go) et un modèle d'abonnement annuel.

New Relic est une plate-forme complète qui offre un bon équilibre entre fonctionnalités, convivialité et évolutivité via son architecture Kafka. La plate-forme suscite beaucoup d'intérêt, ce qui lui donne de nombreuses opportunités sur le marché. Elle semble toutefois s'adresser en particulier aux secteurs des services et de la finance. La compatibilité avec presque toutes les sources de données, associée à des visualisations claires, offrent aux équipes chargées du développement et des opérations tous les outils dont elles ont besoin pour gérer et résoudre les problèmes de performances.

Points forts : les systèmes de visualisation intuitifs offrent un aperçu rapide et facile des systèmes. La surveillance Kubernetes est l'une des meilleures du marché. Les balises permettent de créer des tableaux de bord avec peu d'intervention de l'équipe informatique. La plate-forme est conçue pour évoluer.

Défis : malgré un certain nombre de fonctionnalités IA, New Relic n'offre pas de véritable correction automatique, ce qui pourrait mettre les administrateurs en difficulté en temps de crise.

Splunk

Splunk travaille dans le secteur de la surveillance informatique depuis plus de 15 ans. En 2019, Splunk a fait l'acquisition de SignalFx (entreprise fondée en 2013) et d'Omnition (entreprise fondée en 2018). Ces deux produits ont amélioré la convivialité de la plate-forme Splunk et l'ont transformée en une solution d'observabilité complète.

La solution Splunk combine des solutions de surveillance, de dépannage et de gestion des incidents qui stimulent les initiatives de modernisation des applications. Splunk fait converger la surveillance de l'infrastructure, la surveillance des performances applicatives, la surveillance de l'expérience numérique, les analyses de journaux et la gestion des incidents dans une seule plate-forme.

La solution d'observabilité de Splunk comprend les éléments suivants : Splunk Infrastructure Monitoring (solution de surveillance et de dépannage basée sur des métriques en temps réel), Splunk APM (solution de surveillance et de dépannage des applications basée sur le traçage), Splunk RUM (solution de surveillance et de dépannage des utilisateurs finaux, en version bêta), Splunk Log Observer (solution d'analyse des journaux pour les équipes DevOps, en version bêta), Splunk On-Call (solution de gestion intelligente et collaborative des incidents) et Splunk Observability Mobile (solution d'alertes et de graphiques en temps réel).

Grâce à l'acquisition de Rigor et Plumbr en 2020, l'entreprise propose également Splunk Synthetic Monitoring et Splunk Web Optimization (via Rigor), ainsi que l'instrumentation de bytecode (via Plumbr), actuellement en version bêta. Le composant Service Bureau qui permet aux fournisseurs de services d'afficher les jetons/quotas pour la visibilité et le contrôle de l'utilisation et de l'allocation constitue une autre fonctionnalité utile. La solution fournit également des bonnes pratiques partageables, telles que le tableau de bord et les alertes.

L'architecture NoSample utilise des données hautement fidèles à tout moment pour fournir des résultats de meilleure qualité, et la fonction Real-Time Streaming traite toutes les données dès leur entrée pour améliorer le délai moyen de résolution. La plate-forme utilise des fonctions IA et ML pour faciliter et guider l'identification et la correction des erreurs.

La solution Splunk dispose d'une large gamme d'intégrations pour faciliter l'analyse et la résolution des causes premières, telles que ServiceNow, IBM Z Decision Support, Jira, SolarWinds, Git, Jenkins, Spinnaker, GitLab et CircleCI. Le système offre un large choix de visualisations, ainsi qu'un accès facile aux journaux, aux métriques et aux traces pour faciliter le diagnostic et la remédiation.

La plate-forme offre des moyens simples d'augmenter ou de réduire la capacité opérationnelle, et simplifie la détection et la correction des menaces. La plate-forme est particulièrement adaptée aux moyennes et grandes entreprises.

La gamme Splunk Observability Suite est une offre SaaS avec un modèle basé sur un abonnement. Il existe deux modèles de tarification, un modèle basé sur l'hôte et un modèle basé sur l'utilisation, et deux éditions, Standard et Enterprise. L'édition Enterprise offre des fonctionnalités améliorées de gestion centralisée et de dépannage axé sur les fonctions IA/ML (telles que Service Bureau). Splunk On-Call offre une tarification basée sur l'utilisateur et trois éditions : Starter, Growth et Enterprise. Les clients peuvent payer au mois ou à l'année.

Splunk s'est imposé comme l'un des leaders du marché de l'observabilité avec des acquisitions stratégiques et le développement de solutions internes spécialisées. Bien que la plate-forme de données NoSample constitue un avantage notable, elle pourrait submerger certaines grandes entreprises numériques si ces dernières venaient à collecter toutes les données disponibles sans indexation correcte des balises ou sans réduire la taille des données.

Splunk s'efforce activement de convertir ses clients existants par le biais d'incentives. L'entreprise affirme également qu'elle s'est engagée à s'intégrer à l'ensemble de l'écosystème. Un tel effort permettrait de dissiper les inquiétudes que nous avons entendues sur le terrain au sujet de l'engagement de Splunk en matière d'interopérabilité. L'option d'instrumentation basée sur le service OpenTelemetry de Splunk (via Omnition) permet aux magasins cloud natifs de se développer rapidement avec une option de conversion à l'échelle de l'entreprise.

Points forts : Splunk ingère, avec une fidélité optimale, les données provenant de toutes les sources (journaux, métriques et traces) sur l'ensemble de la pile. La solution offre également une évolutivité massive, des analyses en continu sophistiquées et la prise en charge native d'OpenTelemetry.

Défis : certains clients ont exprimé des inquiétudes quant au coût et à la difficulté potentielle de la migration vers la gamme Splunk Observability Suite. Même à prix réduit, la charge de coût globale de la solution pourrait être supérieure à la moyenne ou coûteuse à long terme par rapport aux autres fournisseurs évalués.

StackState

Fondé en 2015, StackState a son siège social à Utrecht, aux Pays-Bas, et dispose d'un bureau à Boston. Cette start-up agile a conçu sa solution d'analyse des données d'observabilité à partir de zéro et a publié la version actuelle (4.2) de sa solution en décembre 2020. L'entreprise fournit généralement une mise à jour tous les trimestres. Elle offre quelques caractéristiques uniques qui ont trouvé une applicabilité de niche auprès de clients du secteur bancaire et financier, la plupart résidant en Europe.

StackState constitue une solution d'observabilité basée sur la topologie et les relations qui permet de mapper les services métiers sur ses applications, ses dépendances d'infrastructure, sa configuration et ses modifications. Les relations de topologie sont généralement extraites d'un stockage CMDB, tel que BMC Remedy, ServiceNow et les autres outils de gestion informatique. La solution collecte les données en s'intégrant à d'autres outils de surveillance tiers, tels que Splunk, et peut être étendue avec les agents de la plate-forme.

La topologie interdomaine et temporelle de StackState améliore les systèmes existants de surveillance et de résolution des problèmes. La solution fournit un tableau de bord convivial qui affiche non seulement l'état actuel du système, mais propose également une fonction temporelle pour observer l'état précédent des systèmes. Cette fonctionnalité est basée sur StackGraph, une base de données propriétaire de graphiques distribués avec versions gérées, en plus de HBase/Hadoop, et prend en charge des systèmes de télémétrie virtuelle tels qu'Elasticsearch, Splunk, Prometheus, CloudWatch et Azure Monitor.

La plate-forme assure une prise en charge cloud native de Kubernetes, EKS, AKS, ECS et OpenShift, Docker et Docker Swarm. StackState peut intégrer automatiquement la topologie et la télémétrie à partir de solutions basées sur vSphere et dispose également d'un SDK ouvert capable de prendre en charge les solutions d'ancienne génération.

La plate-forme dispose d'une couche de virtualisation en plus des lacs de données, ou data lakes, qui lie automatiquement les références de télémétrie à la topologie. Elle prend en charge les formats de traçage OpenTracing, Datadog, AWS CloudWatch et Jaeger.

StackState dispose d'un système de détection des anomalies entièrement autonome qui utilise des points de référence pour tous les environnements. La solution est capable d'identifier les glissements au fil du temps et dans des conditions de contrainte. Elle peut également déclencher des actions définies pour différentes situations, ainsi que des corrections automatisées.

Le tableau de bord de la carte topologique basée sur les relations constitue une fonctionnalité très conviviale qui montre l'état des systèmes et identifie les services qui ne se comportent pas correctement en les affichant en rouge. Le rapport de cumul vers un service métier affecté, basé sur le modèle extrait de CMDB, permet de visualiser les systèmes métiers affectés, tels que les services bancaires en ligne.

Les modifications de configuration et les systèmes de gestion des modifications peuvent fournir des informations, ce qui peut s'avérer utile lorsque vous utilisez la fonction temporelle sur la carte topologique pour trouver un incident spécifique et sa cause. La fonction Automated Root Cause Analysis de StackState identifie la cause première. Elle permet d'examiner les données sous différents angles pour effectuer manuellement une analyse des causes premières et suggérer ou effectuer des corrections.

Cette solution est un outil léger disponible pour un déploiement SaaS ou sur site.

Solution d'analyse des métriques, StackState s'intègre à d'autres outils de surveillance pour les informations sur les métriques. Pour devenir une plate-forme d'observabilité complète, StackState doit améliorer la télémétrie et la gestion des signaux. L'observabilité ne doit pas uniquement répondre à la question « quand », mais aussi aux questions « quoi » et « comment ». Les différentes parties de cette solution couvrent l'observabilité (identification des incidents basée sur la topologie), AIOps (détection des anomalies) et DevOps (gestion des changements, effets CMDB déclenchés par les changements apportés aux systèmes de production).

Points forts : StackState propose une vue basée sur le profil destinée aux services informatiques/services professionnels qui est conviviale et facilite l'affichage des vues dans un contexte spécifique tout en permettant d'utiliser la fonction temporelle pour visualiser la topologie menant à l'état actuel. L'intégration CI/CD et CMDB est un concept intéressant. Le système peut identifier les problèmes causés par les modifications au lieu de symptômes ; ainsi, le service peut être rapidement isolé, un vrai avantage pour les cas d'utilisation DevOps.

Défis : StackState doit améliorer la télémétrie et la gestion des signaux. L'efficacité du système dépend grandement de la qualité des données des systèmes sous-jacents, de CMDB et des fournisseurs de données (comme Splunk, par exemple).

Sumo Logic

Sumo Logic est une plate-forme d'observabilité SaaS mutualisée et cloud native. Elle a été conçue à l'origine comme solution de gestion des journaux, d'analyse de big data et de gestion des informations et des événements de sécurité (SIEM, Security Information and Event Management). Aujourd'hui, Sumo Logic a ajouté des fonctions de suivi et de métriques pour transformer le produit en une plate-forme d'observabilité complète.

La plate-forme Continuous Intelligence Platform™ de Sumo Logic ingère et analyse des données provenant d'applications, d'infrastructures, de données de sécurité et de sources IoT. Elle développe ensuite des analyses unifiées en temps réel. La plate-forme utilise les fonctions IA/ML pour créer une expérience utilisateur fluide lors de l'exploration des journaux, des métriques et des traces.

La plate-forme est dotée d'intégrations prêtes à l'emploi pour AWS, Telegraf, Kubernetes et Prometheus. Elle peut utiliser une combinaison de plusieurs bases de données backend selon le déploiement, y compris DynamoDB et S3. Ses outils de diagnostic sont assistés par ML et son interface utilisateur offre plusieurs moyens d'accéder aux informations stratégiques.

Les utilisateurs peuvent créer des tableaux de bord pour chaque microservice et afficher instantanément l'ensemble des métriques, traces et journaux associés. Les visualisations de ces éléments, assistées par les processus IA, favorisent une navigation rapide et facile, et permettent aux ingénieurs de diagnostiquer les causes des erreurs et des défaillances.

Ce service cloud natif mutualisé inclut également les fonctions Root Cause Explorer et Global Search, un moteur de comparaison temporelle et spatiale, ainsi que la fonction Outlier Detection pour calculer en continu plusieurs références.

La solution Continuous Intelligence Platform de Sumo Logic convient particulièrement aux moyennes et grandes entreprises qui cherchent à faire évoluer leurs capacités d'observabilité et à fournir à leurs ingénieurs une solution complète pour résoudre rapidement et efficacement les interruptions de service.

La solution utilise un système de paiement unique basé sur les « crédits cloud ». Les utilisateurs achètent un certain nombre de crédits et peuvent accéder à l'ensemble de la plate-forme en utilisant ces crédits pour différentes fonctionnalités. Les coûts sont liés à la quantité de données ingérées et peuvent facilement évoluer à la hausse ou à la baisse, selon les besoins du client.

La solution Continuous Intelligence Platform offre également de nouvelles fonctionnalités d'observabilité via sa plate-forme de gestion des journaux dont l'interface utilisateur conviviale permet une investigation plus approfondie des problèmes et donc un diagnostic rapide. Le manque de correction automatique pourrait être considéré comme une faiblesse, mais ses nombreuses intégrations permettent d'atténuent ce facteur.

Points forts : le tableau visuel affichant les indicateurs clés de performance de l'entreprise et les métriques concernées identifie les systèmes critiques affectés et les pertes de revenus potentielles. La budgétisation permet aux clients de spécifier exactement la quantité de données qu'ils souhaitent traiter et de limiter leur consommation. Le nouveau modèle de tarification fixe basé sur le volume de données pourrait rendre cette solution plus attrayante pour les entreprises soucieuses de leurs budgets.

Défis : cette solution n'est pas optimisée pour les installations de cloud privé sur site. Les entreprises basées sur Azure et GCP, ainsi que les grands utilisateurs de solutions sans serveur, pourraient rencontrer des problèmes avec Sumo Logic au niveau de la collecte et de l'hébergement des données. La solution manque de fonctions de surveillance de l'utilisateur/de l'expérience, de surveillance synthétique, et de surveillance et de métriques au niveau des applications natives mobiles, des composants essentiels d'une solution d'observabilité complète.

VMWare Tanzu Observability

La suite de solutions VMWare Tanzu, conçue pour prendre en charge le cloud, le cloud hybride et les applications conteneurisées, inclut désormais la plate-forme d'observabilité Tanzu Observability. VMWare étend sa prise en charge du cloud et de Kubernetes. Cette plate-forme, dont le produit d'origine, Wavefront, a été renommé en mars 2020, vise à produire, assurer la gestion et faire évoluer des applications cloud natives.

La solution Tanzu Observability est spécialement conçue pour aider les entreprises à surveiller, observer et analyser les applications et les environnements cloud natifs. Elle utilise des métriques, des traces, des histogrammes, des journaux de délai et des événements. Ces données sont extraites des applications distribuées, des services applicatifs, des services de conteneur, ainsi que des infrastructures de cloud public, privé et hybride pour créer une image en temps réel d'un écosystème complet.

Tanzu Observability offre un rendu instantané des graphiques et une mise à jour en temps réel, ce qui permet un triage itératif rapide des incidents. Les utilisateurs peuvent créer et personnaliser des tableaux de bord à partir d'un ensemble d'outils simple et compatible avec l'utilisation de widgets. Les tableaux de bord peuvent être en libre-service et utilisés par des milliers d'utilisateurs au sein d'une entreprise.

Les intégrations de surveillance prêtes à l'emploi incluent Dynatrace, Grafana, Graphite, Nagios, New Relic, Prometheus, Sensu, Splunk, vRops et Zabbix. La solution assure la mise en corrélation des données entre les applications, l'infrastructure, les développeurs et les outils DevOps d'une part, et les packages, les tableaux de bord, les métriques et les alertes, d'autre part.

La plate-forme offre plus de 100 fonctions analytiques permettant de naviguer et d'isoler les problèmes de production. En matière de détection des anomalies, Tanzu Observability utilise AI Genie, un outil automatique de détection des anomalies et de prévision basé sur les fonctions IA/ML. Les utilisateurs peuvent créer des alertes intelligentes pour filtrer les événements non critiques et capturer les anomalies dans différents environnements et périodes. Les utilisateurs peuvent également afficher et mettre en corrélation des événements (activités de déploiement, démarrage de la fenêtre de maintenance, etc.) et des alertes sous forme de superpositions dans la vue de métriques de leur choix.

Particulièrement adaptée aux grandes entreprises, la solution Tanzu Observability est utilisée par de nombreuses organisations dans le secteur des services. La tarification est basée sur la consommation et utilise le taux mensuel de données de métriques fournies. Les clients disposent ainsi de flexibilité et peuvent commencer avec n'importe quelle taille d'application, puis monter ou baisser en gamme selon leurs besoins. La tarification ne dépend pas du nombre d'hôtes ou d'utilisateurs.

VMWare a créé une suite d'observabilité complète et robuste. Bien que la solution dispose de fonctionnalités d'entreprise solides telles que la gouvernance, la sécurité, l'utilisation de stratégies et la conformité, elle aurait tout avantage à suivre la voie de certaines des nouvelles plates-formes d'observabilité numérique pour offrir davantage de solutions cloud natives. La solution pourrait également améliorer le processus de rétrofacturation et les contrôles de stratégie de déploiement basés sur la conformité. Sur une note similaire, l'instrumentation automatique ou une instrumentation plus rapide serait une amélioration appréciée.

Points forts : VMWare est l'un des rares fournisseurs à considérer les machines virtuelles, les logiciels d'entreprise et les solutions cloud natives comme des éléments à part entière. Il est plus facile de créer un véritable système d'observabilité multicloud à l'aide de VMWare. La solution permet également d'observer les clusters Kubernetes exécutés sur n'importe quel type d'infrastructure cloud AWS, Azure, GCP et sur site.

Défis : les cycles de validation de principe et de mise en œuvre semblent être plus longs pour de nombreuses entreprises. Le délai de retour sur investissement est supérieur à celui des autres fournisseurs du secteur. C'est également l'une des solutions les plus coûteuses de ce segment de marché. La plupart des autres fournisseurs réévaluent leurs tarifs pour rester compétitifs.

Zebrium

Fondée en 2017, l'entreprise Zebrium, basée à Santa Clara en Californie, a lancé ses services en disponibilité générale en 2020, ce qui en fait une nouvelle venue sur le marché de l'observabilité. Sa solution repose sur l'analyse automatisée des causes premières et la détection des incidents à l'aide des fonctions IA/ML sur les journaux et les métriques, ce qui permet aux équipes chargées des opérations informatiques de réduire le délai moyen de résolution.

Zebrium est une plate-forme AIOps/d'observabilité qui utilise le machine learning non supervisé pour détecter automatiquement les problèmes logiciels et en trouver automatiquement la cause première. Le système ne nécessite pas de configuration manuelle. Il s'entraîne sur la topologie de l'entreprise en établissant des références à tous les niveaux de l'infrastructure et est capable de détecter les incidents en une journée.

Le système aide non seulement les utilisateurs humains à diagnostiquer la cause première des problèmes, mais il détecte également de manière proactive les problèmes et envoie aux ingénieurs des rapports de cause première décrivant le problème, l'endroit où il s'est produit et le moment où il s'est produit. Le machine learning non supervisé comporte également une fonction qui permet à un utilisateur humain d'accepter, de désactiver ou de rejeter les résultats comme étant vrais ou non. Le système utilise ensuite l'apprentissage par renforcement pour affiner son algorithme sans intervention manuelle supplémentaire.

Zebrium travaille presque exclusivement avec les journaux et les métriques (les traces ne sont pas prises en charge pour le moment) pour effectuer la détection et le diagnostic. La solution possède un collecteur natif et prend entièrement en charge Kubernetes (y compris des variantes comme OpenShift). Elle dispose également d'un collecteur natif pour Docker et Linux et prend en charge la collecte de journaux via logstash ou syslog pour Windows, VMWare et la plupart des autres environnements. Zebrium a construit une fonction Lambda pour le transfert de journaux (une fonction semblable à Amazon CloudWatch). La plate-forme n'utilise pas de données échantillonnées et peut gérer l'acquisition de données à grande échelle de l'ordre du pétaoctet.

La plate-forme peut ingérer et analyser toutes les données, y compris les données non structurées, ce qui est particulièrement utile pour les journaux. Son machine learning automatique apprend les structures des événements de journaux et recherche les hotspots des modèles anormalement corrélés pour détecter les incidents réels sur les signaux anormaux de base. En mettant en corrélation les journaux provenant de plusieurs sources avec les données de métriques, Zebrium peut créer de manière proactive des rapports d'incident réels, y compris des détails sur la cause première potentielle, sans intervention manuelle.

Grâce à la technologie Zebrium, les clients types peuvent réduire le délai moyen de résolution d'un incident logiciel de quelques heures à quelques minutes. La solution utilise la pile ELK pour la recherche, la collecte de données et la gestion des journaux.

Zebrium se présente sous la forme d'une solution SaaS mutualisée qui peut être déployée sur un VPC appartenant au client ou installée sur site. La solution bénéficie d'un essai gratuit, et la configuration est assez facile et rapide. La solution est facturée en fonction du volume de données et la plate-forme peut être installée sur site pour les clients plus importants.

La plate-forme peut être utilisée avec tout produit de surveillance informatique actuellement disponible sur le marché en se connectant à la solution et en signalant automatiquement les problèmes et les détails de la cause première au centre d'opérations réseau (NOC) ou au centre d'opérations de sécurité (SOC).

Il s'agit d'un début très prometteur pour cette start-up, en particulier avec l'utilisation des fonctions IA/ML pour différencier les incidents réels de la pile d'anomalies. Actuellement, la solution utilise uniquement les journaux et les métriques, mais devrait prendre en charge les traces à l'avenir.

Points forts : le machine learning de Zebrium trouve automatiquement la cause première des incidents sans nécessiter de recherche manuelle dans les journaux et les métriques. La solution peut également détecter de manière proactive les anomalies dans les journaux et les métriques sans création manuelle de règles. En outre, elle peut potentiellement réduire l'accoutumance aux alertes en identifiant uniquement les incidents que le système estime réels.

Défis : bien que le système soit hautement précis, il existe un risque de faux négatifs qui pourraient dissimuler des incidents réels. Les faux positifs constituent également un risque lorsqu'un changement se produit dans le système. Pour que ce système IA/ML fonctionne correctement, les deux signaux (journaux et métriques) doivent être puissants. Seuls deux cas d'utilisation sont actuellement pris en charge : la recherche automatique de la cause première des incidents et la détection proactive des nouveaux incidents.

6. Point de vue de l'analyste

L'évaluation d'un outil dans un secteur d'activité émergent, tel que l'observabilité cloud, constitue toujours un défi de taille, en particulier lorsqu'il existe une diversité de solutions répondant aux approches cloud uniquement, cloud hybride et multicloud. Lors de notre processus de présélection des meilleurs fournisseurs, nous avons découvert un marché robuste et en évolution rapide, avec des solutions présentant différents points forts et points faibles. Bien que la plupart des fournisseurs proposent des solutions solides dans ce domaine, de nombreuses caractéristiques futuristes sont encore attendues.

- **Correction automatique/autoréparation :** l'objectif ultime de l'observabilité est de minimiser les temps d'arrêt, de créer des systèmes robustes et de réduire au maximum le délai moyen de résolution. L'identification et la mise à disposition d'informations ne suffisent pas. Les solutions doivent automatiser au moins les corrections de base pour éliminer les interventions humaines coûteuses.
- **Connectivité ouverte :** nous avons constaté qu'aucune solution ne peut répondre de manière optimale à l'ensemble des besoins en matière d'observabilité. Ainsi, la prise en charge d'une connectivité ouverte, pour la collecte, le traçage ou l'automatisation de la télémétrie, s'avère être un atout essentiel pour les entreprises qui souhaitent créer des plates-formes de pointe.
- **Intégration DevOps et CI/CD :** nous espérons voir une intégration plus étroite au cycle et aux outils DevOps pour témoigner du fait que les modifications de code et de configuration représentent la majorité des incidents dans les environnements de production. L'analyse des risques liés aux changements de code avant le déploiement, la restauration automatique des environnements Canary et bleu/vert, ainsi que l'analyse des interruptions potentielles et des pertes d'opportunités commerciales représentent autant de cibles intéressantes pour les systèmes d'observabilité de demain.
- **Analyse de simulation et test de contrainte :** parmi les autres améliorations, il convient de mentionner l'analyse de simulation et les tests de contrainte combinés à des outils de test avant le déploiement.
- **Coût de possession :** les entreprises qui adoptent des plates-formes d'observabilité font face à un problème majeur : en effet, le coût de possession subit l'impact négatif des modèles de tarification des fournisseurs qui manquent trop souvent de transparence. La dépendance vis-à-vis des fournisseurs devient également une problématique essentielle lorsqu'une entreprise s'engage sur une plate-forme unique. Pour résoudre ce problème, nous espérons voir une intégration, une connectivité et une télémétrie plus ouvertes, ainsi qu'une tarification basée sur la consommation, remplaçant potentiellement la tarification basée sur les hôtes, les agents et les systèmes.
- **Utilisation de technologies d'IA réelles :** dans notre analyse, la plupart des fournisseurs utilisent des modèles ML de base pour l'observabilité et pour les cas d'utilisation AIOps. Les technologies d'IA plus sophistiquées, telles que le traitement du langage naturel, le deep learning, les fonctionnalités de réseau de neurones, l'apprentissage supervisé/partiellement supervisé et l'apprentissage par transfert sont prometteuses, bien que leur emploi soit encore en voie de développement. Une autre cible à privilégier est l'analyse des journaux non structurés, un secteur où la plupart des systèmes d'observabilité rencontrent des difficultés. Il s'agit d'un problème courant avec la fonctionnalité de

lecture des journaux d'application et de niveau de service non structurés.

- **Cas d'utilisation professionnel :** alors que la plupart des fournisseurs placent les cas d'utilisation informatique au cœur de leurs activités, peu se concentrent sur les indicateurs clés de performance de l'entreprise. Un utilisateur professionnel devrait être en mesure d'afficher une liste de niveaux d'application métier et de définir la criticité, le coût d'opportunité, ainsi que les contraintes et les coûts autorisés. Il reste beaucoup de chemin à parcourir dans ce domaine, mais il est très intéressant de voir de nombreux fournisseurs travailler au développement d'une solution d'observabilité complète plutôt qu'une approche cloisonnée. Les nouveaux fournisseurs font preuve de beaucoup d'énergie créative et d'innovation, et définissent les exigences en matière de cas d'utilisation et de facilité d'utilisation qui font avancer la technologie.

Au final, le cloud offre de nombreuses opportunités aux fournisseurs dont les solutions innovantes, agiles et rentables permettent de rivaliser avec les géants du marché. Bien que certains de ces nouveaux acteurs manquent de maturité, de sécurité, de gouvernance et du caractère professionnel des solutions établies, ils compensent cette différence grâce à des fonctionnalités ciblées et des approches inspirantes. La clé, comme toujours, consiste à identifier et à sélectionner la solution qui répond le mieux à vos besoins spécifiques.

7. À propos d'Andy Thurai

Expert en informatique et en stratégie, consultant et porte-parole aguerri, Andy Thurai cumule plus de 25 ans d'expérience à des postes de responsable exécutif, technique et d'architecture dans des entreprises telles qu'IBM, Intel, BMC, Nortel et Oracle. Il conseille également de nombreuses start-up. Il a été intervenant principal lors de grandes conférences et a présenté de nombreux webcasts, podcasts, webinaires et chats vidéo. Andy a rédigé plus de 100 articles sur les technologies émergentes pour des médias tels que Forbes, The New Stack, AI World, VentureBeat et Wired.

Les domaines de prédilection d'Andy sont notamment l'AIOps, l'ITOps, l'observabilité, l'intelligence artificielle, le machine learning, le cloud, l'edge computing et d'autres logiciels d'entreprise. Son point fort consiste à vendre la technologie aux équipes de direction en se basant sur une proposition de valeur plutôt que sur un argumentaire technologique.

Pour en savoir plus sur Andy et découvrir certaines de ses publications, consultez son site Web www.thefieldcto.com.

8. À propos de GigaOm

GigaOm fournit des conseils techniques, opérationnels et commerciaux dans le cadre d'initiatives commerciales et informatiques stratégiques auprès d'entreprises numériques. Les chefs d'entreprise, les directeurs informatiques et les organisations technologiques font appel à GigaOm pour obtenir des conseils pratiques, exploitables, stratégiques et visionnaires afin de moderniser et transformer leurs activités. La contribution de GigaOm permet aux entreprises de rester compétitives dans un environnement commercial de plus en plus complexe qui exige une solide compréhension des demandes des clients en constante évolution.

GigaOm travaille directement avec les entreprises, au sein et en dehors du service informatique, pour mettre en œuvre des techniques de recherche et des méthodologies éprouvées conçues pour éviter les pièges et les obstacles tout en équilibrant les risques et l'innovation. Les méthodologies de recherche incluent, sans s'y limiter, des enquêtes d'adoption et d'analyse comparative, des cas d'utilisation, des entretiens, le calcul du retour sur investissement/coût total de possession, les périmètres du marché, des tendances stratégiques et des points de référence techniques. Nos analystes travaillent depuis plus de 20 ans au service d'un large éventail de clients, d'utilisateurs de la première heure aux grandes entreprises.

GigaOm adopte le point de vue d'un expert professionnel impartial. Grâce à cette approche, GigaOm peut collaborer de manière étroite avec des abonnés fidèles et engagés.

9. Copyright