CASE STUDY

INFORMATIONS SUR L'ENTREPRISE :

Le premier prestataire mondial de solutions intégrées de gestion des voyages, des dépenses et de la facturation pour les entreprises et les organismes gouvernementaux.

BESOINS DE L'ENTREPRISE :

- Proposer des applications financières sécurisées dans le monde entier
- Garantir la disponibilité d'une plateforme toujours disponible
- Déployer des applications rapidement et de manière sécurisée pour rester compétitive

DÉFIS :

- Prometheus était un fardeau opérationnel
- Le traitement manuel exigeait une équipe conséquente et ralentissait les activités
- Le manque de données pour la résolution des problèmes et les audits de conformité devenait pénalisant

IMPACT BUSINESS DE SYSDIG :

SAP Concur offre une plateforme globale toujours disponible qui répond aux exigences de sécurité et de conformité. Les nouveaux services arrivent plus rapidement sur le marché.

AVANTAGES DE LA PLATEFORME SYSDIG :

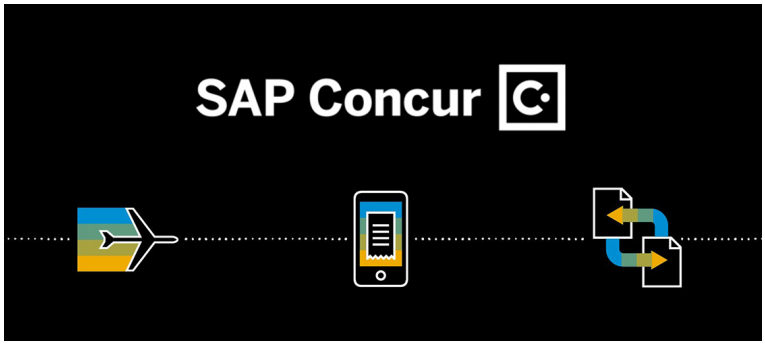
- L'automatisation permet de gagner énormément de temps
- L'approche Secure DevOps, agent unique est plus efficace
- L'analyse des incidents, même lorsque les conteneurs ont disparu
- La plateforme s'adapte à la croissance des clusters Kubernetes - 20 fois plus importante depuis sa création
- L'intégration et la centralisation des logs d'audit pour en faciliter l'analyse

INFRASTRUCTURE :

Amazon Web Services (AWS) et on-premise

ORCHESTRATION :

Kubernetes



SAP Concur offre des solutions sécurisées et conformes à plus de 50 millions d'utilisateurs finaux dans le monde entier

Présentation

SAP Concur est une entreprise de SaaS qui propose des services de gestion des voyages, des dépenses et de la facturation pour les entreprises et les organismes gouvernementaux. Avec une clientèle potentielle globale qui comprend plus de 25 000 PME rien qu'en Amérique du Nord, SAP Concur est à la tête d'une importante infrastructure. Le lancement de nouveaux services fiables et toujours disponibles, de la manière la plus sécurisée possible, est essentiel pour l'entreprise.

SAP Concur a décidé de passer d'une architecture monolithique à la mise en place de microservices pour gagner en flexibilité et proposer des applications plus rapidement. Quatre ans après cette nouvelle orientation, SAP Concur possède une équipe de 20 personnes chargées de gérer un écosystème de conteneurs composé de plus de 2 000 nœuds en production.

Défi

La mise en place de microservices au sein de SAP Concur a commencé grâce à une petite équipe d'intervention

spécialisée, comme l'explique Mike Luedke, directeur de l'ingénierie chez SAP Concur : « Tout est né d'une initiative locale. Nous étions quelques membres issus de différentes équipes et nous avons commencé à construire un cluster. Nous avons fini par élargir ce projet pour inclure les premiers utilisateurs chez Concur. Et puis ça a pris de l'ampleur assez rapidement. Nous sommes partis de ce groupe informel responsable de cette initiative et il est devenu évident qu'elle allait vraiment avoir un impact sur Concur. C'est à ce moment-là que nous avons commencé à mettre en place une équipe officielle pour s'en occuper. »

Étant donné l'origine du projet, toutes les données de la pile de SAP Concur étaient en open source. Au fil du temps, l'équipe a engagé une équipe de sécurité qui a rapidement identifié des failles de sécurité et un manque de visibilité, notamment en comparant la sécurité de l'infrastructure traditionnelle et celle du nouvel environnement de conteneurs.

Selon Luedke, « nous avons atteint un point d'inflexion lorsque nous sommes arrivés à 100 nœuds avec le logiciel open source Prometheus. Il nous fallait trouver une meilleure stratégie de développement. Nos ressources étaient limitées. Nous étions tellement occupés à développer notre projet et à répondre à la demande de nos équipes d'applications internes que nous n'avions pas vraiment assez de temps pour réfléchir au déploiement de Prometheus. Nous avons donc commencé à envisager des options commerciales. »

Raisons pour lesquelles SAP Concur a choisi Sysdig

Luedke explique que, au moment d'envisager différentes options, « Concur a passé pas mal de temps à réfléchir à la solution commerciale qu'il allait intégrer dans sa pile, car c'était le seul élément de notre pile qui était commercial. Tout le reste était en open source gratuit. »

Après avoir comparé les outils commerciaux de surveillance et de sécurité, SAP Concur a choisi Sysdig pour ses nombreux atouts :

- Approche de la sécurité intégrée à Kubernetes
- Reposant sur une approche Open Source (Falco)
- Une approche basée sur les appels systèmes, unique sur le marché
- Sécurité, conformité et surveillance unifiées
- Assistant de création de requêtes PromQL
- Indicateurs détaillés prêts à l'emploi au niveau du noyau, qui peuvent être décomposés selon les besoins

Des milliers d'heures économisées et des livraisons de code quotidiennes

Avant d'utiliser Sysdig, SAP Concur effectuait des révisions manuelles avant de livrer le code dans un environnement de production. Luedke explique que « grâce à Sysdig, nous avons pu automatiser un grand nombre de révisions manuelles. Nous avons intégré Sysdig à nos pipelines où il vérifie la vulnérabilité et la conformité des conteneurs au moment où ils rejoignent notre environnement de production. Ces vérifications automatisées nous permettent d'avancer plus rapidement. »

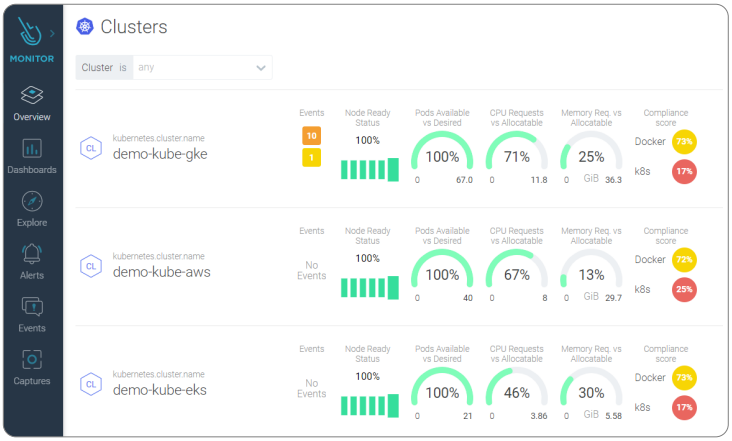
Luedke poursuit son explication du processus de révision et imagine ce que cela impliquerait sans Sysdig dans les conditions actuelles : « Une révision manuelle de ces vulnérabilités ou un traitement manuel prendrait 10 minutes par vérification. Notre précédente option de traitement des vulnérabilités utilisait l'outil open source Clair. Mon équipe devait par conséquent vérifier les résultats dans une autre interface, ce qui prenait du temps. Avec Sysdig, tout

ce processus a pu être automatisé dans le cadre des pipelines tandis que l'équipe procède à leur déploiement. Actuellement, nous traitons des milliers de fusions chaque jour. Si l'on suppose qu'il faut en moyenne 10 minutes pour traiter chacune d'entre elles et que l'on en traite des milliers chaque jour, on n'aurait jamais pu atteindre le même niveau de performance sans Sysdig. »

Supprimer les lacunes en matière de sécurité et de visibilité

Seule plateforme unifiée de sécurité, conformité et surveillance, Sysdig offre un environnement unifié pour éliminer les silos d'information entre les équipes chargées du développement, du DevOps et de la sécurité. Cette approche permet à l'entreprise de résoudre les problèmes plus rapidement

> **« Une révision manuelle de ces vulnérabilités ou un traitement manuel prendrait 10 minutes par vérification. Avec Sysdig tout ce processus a pu être automatisé dans le cadre des pipelines tandis que l'équipe procède à leur déploie- ment. Actuellement, nous traitons des milliers de fusions chaque jour. on n'aurait jamais pu atteindre le même niveau de performance sans Sysdig. »**



en analysant les données précises du système automatiquement corrélées au contexte du cloud ou Kubernetes. Elle donne également la possibilité aux équipes du DevOps d'assumer des responsabilités de sécurité.

De nombreuses équipes de SAP Concur utilisent Sysdig, notamment celles chargées des applications, des opérations, des infrastructures, du DevOps et de la sécurité. Le recours à un outil unique pour de multiples cas d'utilisation a permis à tous les acteurs d'assumer la responsabilité de la sécurité et d'adopter un DevOps sécurisé. À ce sujet, Luedke explique que « grâce à Sysdig, nos développeurs d'applications bénéficient d'un accès direct aux activités en cours. Ils peuvent observer des données telles que les indicateurs de performance et utiliser Sysdig comme un outil de dépannage. Cela leur permet de mettre en place leur propre DevOps sur leurs applications. Il leur suffit d'aller sur Sysdig et de jeter un œil aux activités en cours sans avoir à contacter l'équipe des opérations ou l'équipe chargée des infrastructures. »

Mike explique également que « Sysdig fait gagner du temps à tout le monde, aux développeurs d'applications tout comme à l'équipe chargée des infrastructures. Et c'est pour cela qu'il permet aux utilisateurs

de poser plein de questions, car ils consultent plus fréquemment ces données. Une telle visibilité facilite les choses. Il n'y a pas de frais supplémentaires ; quand ils veulent consulter des données, rien ne les empêche de le faire. Je pense que cela nous permet d'être plus conscients de ce qui se passe dans notre infrastructure. »

Mike indique également que la plateforme unifiée leur offre non seulement une plus grande sécurité, mais leur permet également d'économiser des ressources et de l'argent. « Disposer d'une solution unique qui s'intéresse à la surveillance de manière globale est un gage de simplicité. Je veux dire qu'elle permet d'effectuer une surveillance opérationnelle de l'infrastructure, ainsi qu'une surveillance de la sécurité. Ce n'est pas rien ! D'un point de vue tactique, le fait qu'un agent unique rapporte toutes ces données nous permet d'économiser beaucoup d'argent. Chaque agent implique de disposer d'une capacité de traitement, donc il est très appréciable d'y parvenir avec un seul agent. Il nous faudrait deux outils pour obtenir les résultats que nous offre Sysdig, c'est-à-dire que nous devrions avoir deux fois plus d'agents. »

Des indicateurs Prometheus à l'échelle de l'entreprise

Avant d'opter pour Sysdig, l'équipe de SAP Concur utilisait Prometheus pour ses opérations de surveillance. Selon Luedke, « du point de vue des indicateurs, nous n'avions pas trop de problèmes car nous utilisions Prometheus. Par contre, nous rencontrions des difficultés relatives à la flexibilité. Au fur et à mesure que nous nous développions, nous perdions régulièrement notre base de données Prometheus à cause de problèmes d'adaptation. À un moment donné, nous ne pouvions stocker que les données récupérées pendant une heure. Si un problème survenait plus d'une heure avant, nous étions pris au piège car nous avions recueilli trop de données. Parfois, nous perdions la totalité de la base de données et tout plantait. Nous n'avions plus aucune donnée. Nous n'avions aucune visibilité. »

Sysdig est la seule solution intégralement compatible avec Prometheus. Elle inclut une assistance pour le langage de requête de Prometheus (PromQL) qui permet d'effectuer des requêtes métriques avancées, de construire des tableaux de bord et de créer des alertes. Sysdig résoud les problèmes qui empêchent les équipes d'utiliser le service de surveillance Prometheus à l'échelle de l'entreprise : évolutivité, conservation des données et contrôles de l'accès à l'entreprise.

Intégrer la sécurité dès le développement grâce au scan d'images

Les entreprises peuvent gérer les risques inhérents à la sécurité en détectant et en solutionnant les vulnérabilités et les erreurs de configuration à un stade précoce du processus de DevOps grâce au scan des images. SAP Concur utilise Sysdig pour scanner

> **«Nous avons intégré Sysdig à nos pipelines où il vérifie la vulnérabilité et la conformité des conteneurs au moment où ils rejoignent notre environnement de production. Ces vérifications automatisées nous permettent d'avancer plus rapidement. »**

constamment des images stockées dans les registres et pipelines CI/CD, et durant la production. Cela permet de gagner du temps en cartographiant uniquement les vulnérabilités des applications basées sur Kubernetes.

Selon Luedke, « nous comptons sur Sysdig pour scanner les vulnérabilités et détecter les intrusions sur nos conteneurs. Avant Sysdig, nous disposions d'un système de détection des intrusions basé sur l'hôte qui s'exécutait sur nos nœuds, mais il n'y avait aucun contexte. Il nous indiquait éventuellement le processus touché, qui ressemblait simplement à l'identifiant Docker. Dans un grand environnement multi-tenant, nous ne savions absolument pas à quelle application appartenait ce conteneur si nous ne le recoupions pas avec des métadonnées Kubernetes. Nous pouvions bien obtenir ces informations, mais c'était un processus vraiment très compliqué à effectuer quotidiennement. Sysdig nous a permis d'accéder très rapidement aux événements de sécurité et à d'autres informations de bas niveau dans leur contexte. »

« Avec le temps, l'utilisation de Sysdig et la manière dont nous sécurisons l'environnement continue de croître au fur et à mesure que l'entreprise se développe. Autrefois, nous mettions l'accent sur les clients commerciaux, mais maintenant nous avons vraiment développé nos activités dans le secteur public. Cela implique de nouvelles obligations en matière de conformité. Nous avons pu mettre Sysdig à profit pour respecter certaines de ces exigences. À nos débuts, nous procédions à des investigations manuelles une ou deux fois par semaine et devions y consacrer plusieurs heures à chaque fois. Cependant, les exigences de conformité auxquelles nous sommes soumis se sont accrues avec le développement de notre environnement Kubernetes et nous ne pouvions plus utiliser la méthode manuelle. Étant donné notre taille actuelle, nous ne pourrions pas fonctionner sans Sysdig. Nous ne pourrions tout simplement pas utiliser Kubernetes si nous ne disposions pas d'une telle solution. »

Rapports de conformité simplifiés

Grâce à la fonction Activity Audit (audit d'activité), Sysdig recueille les données d'activité des conteneurs et corrèle les informations avec le contexte d'application, ainsi que les utilisateurs ou services de Kubernetes. Cette fonction s'est très souvent révélée utile pour SAP Concur, notamment lors d'audits.

Selon Luedke, « les pistes d'audit nous ont aidés dans d'innombrables situations. Un jour, des auditeurs voulaient s'assurer que nous exécutions bien l'environnement comme nous le prétendions. Ils ont demandé à voir des informations de processus provenant d'un conteneur spécifique qui exécutait une infrastructure, mais ce conteneur exécutait des images légères, donc il n'y avait aucune interface système. C'est très sécurisé car ça se limite à ce qui doit être exécuté, mais cela signifie également que vous ne pouvez pas faire certaines actions comme obtenir les informations de processus en l'exécutant. Nous avons pu utiliser Sysdig pour obtenir une plus grande visibilité de ce conteneur et fournir les preuves aux auditeurs. »

Luedke précise sa pensée : « J'ai tout simplement regardé les tableaux de bord sur l'écran des indicateurs des processus pour ce cas spécifique et je leur ai donné les informations qu'ils souhaitaient. Ils ont également posé des questions pour s'assurer que nos conteneurs étaient immuables, car nous leur avions dit que nous respections cette obligation. Grâce à Sysdig, nous avons pu démontrer que nos conteneurs actifs n'avaient pas été modifiés depuis leur lancement. Nous avons tout simplement utilisé les évènements d'audit de Sysdig pour afficher le système de fichiers et l'activité de l'interface système sur les conteneurs pour le prouver. »

Une investigation même quand les conteneurs n'existent plus

Les mêmes pistes d'audit d'activité utilisées lors des audits de conformité sont très précieuses en cas de comportement anormal. Avec Sysdig, les entreprises peuvent recueillir toutes les informations d'activité dans un fichier de capture à des fins d'investigation, même si le conteneur n'existe plus.

Pour SAP Concur, Luedke explique que « Sysdig nous a aidés, à de nombreuses reprises, à résoudre des problèmes. Nous l'utilisons constamment comme outil de dépannage en cas de panne ou d'altération des services. Sysdig nous aide à identifier l'emplacement des problèmes. C'est l'une des fonctions les plus utiles de Sysdig. »

Selon Luedke, au-delà des captures, « il est incroyablement utile d'être en mesure de décomposer des indicateurs selon différents critères. Nous sommes souvent confrontés à des problèmes uniques et, en l'absence d'une vue prédéfinie qui nous montre le problème comme nous devons le voir, nous pouvons rapidement la créer. Je n'ai pas de mots pour vous décrire l'utilité de cet outil lorsque tout ne se passe pas comme prévu. »

Les données approfondies du Kernel offrent une visibilité sans précédent

Sysdig utilise des appels système pour signaler les activités au sein d'un conteneur. En tant que mécanisme principal de l'interaction entre l'utilisateur et le noyau, les appels système offrent un bon aperçu des activités d'un programme, et peuvent être un outil précieux pour les activités de dépannage, de surveillance et d'identification des goulots d'étranglement.

Luedke confirme : « Nous avons aimé l'approche de Sysdig. Nous avons apprécié ses instruments de mesure et la manière dont ils recueillent réellement les données, des caractéristiques qui en font une excellente solution de surveillance de la sécurité comparée aux autres options disponibles. Les autres outils de sécurité font beaucoup d'extensions résiduelles des fonctions Kubernetes. Elles bouchent les trous avec Kubernetes en quelque sorte. Mais au fur et à mesure que Kubernetes mûrit, ces lacunes sont déjà incluses ou réglées en amont. Nous croyons vraiment en l'extraction des indicateurs à partir du noyau. C'est une stratégie très solide. J'ai toujours été impressionné par les indicateurs prêts à l'emploi fournis par Sysdig. Il s'agit de données de très bas niveau et elles sont très détaillées comparées à d'autres solutions, ce qui nous permet d'avoir une vision très complète des problèmes. »

Disponibilité optimisée dans l'infrastructure de cloud hybride

L'environnement SAP Concur inclut un cloud AWS et une infrastructure locale. Avec Sysdig, SAP Concur bénéficie de la même visualisation sur toutes ses infrastructures, ce qui permet d'anticiper plus facilement les problèmes avec les microservices qui présentent des dépendances entre les plateformes. En cas de problème, la visibilité sur l'ensemble du système peut aider à trouver une solution plus rapidement.

Comme l'explique Luedke, « nous pouvons rechercher des problèmes sur AWS et localement avec une visualisation unique sur Sysdig. La configuration de l'interface nous permet de détecter des anomalies sur l'un ou l'autre de nos environnements assez rapidement. Grâce aux regroupements intelligents sur les tableaux de bord, nous pouvons regrouper différents critères d'indicateurs de manière logique dans le contexte dont nous avons besoin. Je peux examiner et

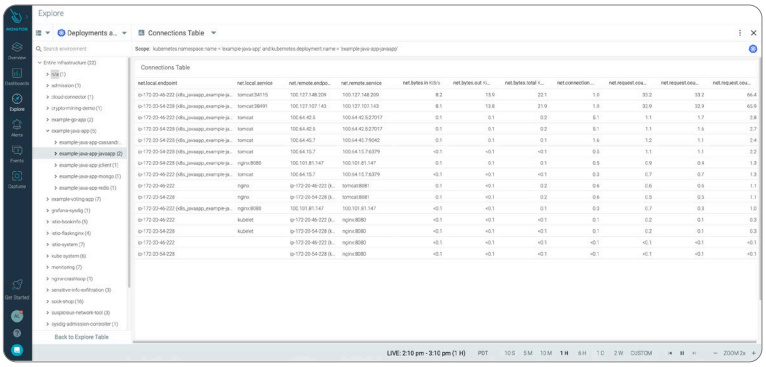
décomposer les données, obtenir la visualisation souhaitée (Kubernetes ou un espace de noms, ou une visualisation plus physique, ou même mon cluster), puis l'inclure au contexte de Sysdig ; tout cela nous permet de comprendre parfaitement ce qui se passe sur la totalité de l'infrastructure. »

Entreprise ouverte, axée sur la communauté

Lorsque SAP Concur en était encore à l'étape de sélection, l'équipe était intéressée par Sysdig car il repose sur une base open source. Selon Luedke, « nous avons aimé la manière dont Sysdig adoptait l'open source et y contribuait. Cet aspect était important à nos yeux. »

Aujourd'hui, l'open source stimule le cloud. Le fait d'être construit sur des outils open source tels que Sysdig Inspect, Falco et Prometheus permet à Sysdig d'avancer plus rapidement tout en proposant un logiciel plus sécurisé.

Pour Luedke, grâce à l'adoption de l'Open Source par Sysdig, il est plus facile d'ajouter de nouvelles fonctionnalités. Selon lui, « il s'est avéré utile d'être en mesure d'utiliser rapidement et facilement des standards Open Sources comme Prometheus. Par



exemple, dans les quelques cas où il n'y a pas eu d'intégration prête à l'emploi, nous avons pu construire ce que nous voulions avec les points de terminaison Prometheus. C'est facile, rapide et vraiment appréciable. »

En tant qu'entreprise basée sur l'open source, Sysdig mise sur la collaboration. Depuis le lancement de Sysdig, l'équipe produit a passé des heures à écouter les clients et à laisser leurs besoins dicter la roadmap. En tant qu'utilisateur de longue date, ce niveau de service était très important aux yeux de Luedke : « Sysdig a été un partenaire de choix pour nous. La société a toujours été à l'écoute de nos besoins au fur et à mesure qu'ils évoluaient, et elle nous a aidé à trouver des solutions à nos problèmes. Sysdig est restée à nos côtés dans toutes les circonstances. »

Pour en savoir plus sur Sysdig, rendez-vous sur www.sysdig.com et pour bénéficier d'un essai gratuit, rendez-vous sur www.sysdig.com/trial.

sysdig

Copyright © 2021 Sysdig, Inc. All rights reserved.
CS-SAPCONCUR-FR Rev. A 10/21