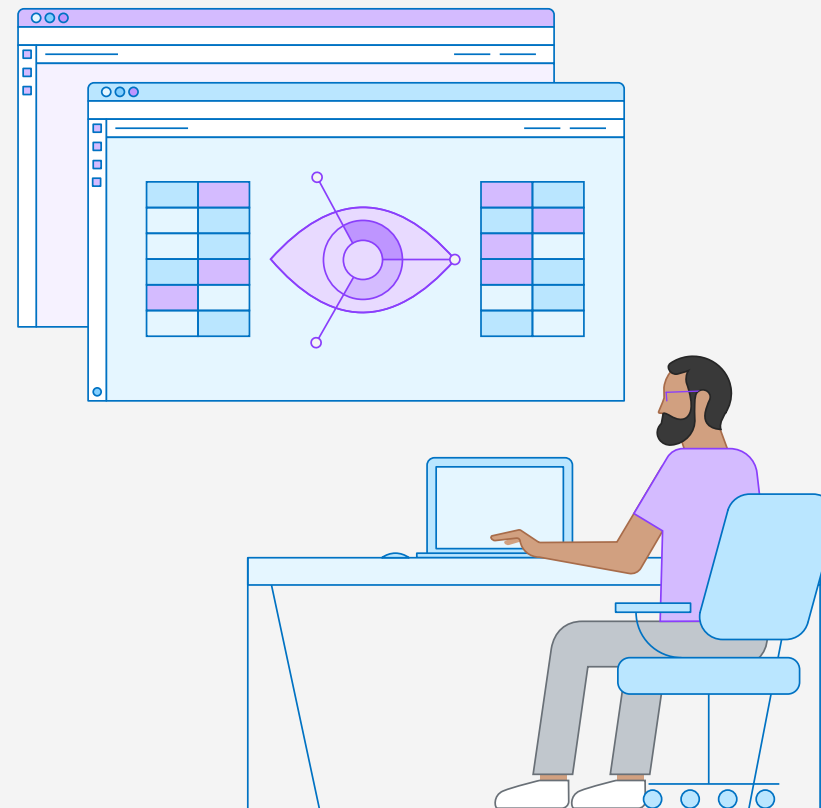




Observabilité et surveillance : quelle est la différence ?

[Commencer ici →](#)



La surveillance et l'observabilité sont deux façons d'identifier les causes sous-jacentes des problèmes. Mais quelles sont leurs similitudes et leurs différences ?

Lorsqu'une application ne fonctionne pas correctement, le dysfonctionnement a un impact sur les clients et, donc, sur l'activité. Les équipes doivent disposer d'outils pour identifier la cause première des problèmes afin de rapidement résoudre ces derniers. C'est là qu'interviennent la surveillance et l'observabilité.

La surveillance et l'observabilité sont deux moyens d'identifier la cause sous-jacente des problèmes. La surveillance signale la survenue d'un dysfonctionnement, tandis que l'observabilité indique ce qui se passe, pourquoi et comment y remédier. Pour mieux comprendre la différence entre l'observabilité et la surveillance, examinons leur fonctionnement et les rôles qu'elles jouent aujourd'hui dans le développement des logiciels.

Qu'est-ce que l'observabilité ?

L'[observabilité](#) est la capacité à comprendre l'état interne d'un système complexe à partir de résultats externes. Lorsqu'un système est observable, un utilisateur peut identifier la cause première d'un problème de performance en examinant les données que le système produit sans test ni code supplémentaire.

Le terme provient de la théorie du contrôle, un concept d'ingénierie qui fait référence à la possibilité d'évaluer les problèmes internes depuis l'extérieur. Par exemple, l'observabilité procurée aux mécaniciens par les systèmes de diagnostic automobile leur permet de comprendre pourquoi votre voiture ne démarre pas sans avoir à la démonter.

En informatique, une solution d'observabilité analyse les données de sortie, évalue la santé du système et fournit des informations exploitables pour résoudre un problème. Un système observable est un système dans lequel les [équipes DevOps](#) peuvent voir l'ensemble de l'environnement informatique dans son contexte et comprendre les interdépendances. Le résultat ? Les équipes sont ainsi en mesure de détecter les problèmes de manière proactive et de les résoudre plus rapidement.

Qu'est-ce la surveillance ?

La [surveillance](#) consiste à évaluer la santé d'un système en collectant et en analysant les données d'agrégation des systèmes informatiques à partir d'un ensemble prédéfini de mesures et de journaux. Dans le domaine du DevOps, la surveillance mesure la santé d'une application, par exemple en créant une règle qui émet une alerte lorsque le taux d'utilisation du disque par l'application approche de 100 %, ce qui permet d'éviter une indisponibilité. Cependant, la vraie valeur de la surveillance se révèle dans l'analyse des tendances à long terme et dans les alertes. En effet, elle indique comment fonctionne l'application, mais également son utilisation dans le temps.

Grâce à la surveillance, les équipes peuvent observer la performance d'un système et détecter les dysfonctionnements connus. Mais la surveillance a ses limites. Pour que la surveillance soit efficace, vous devez connaître les mesures et les journaux à suivre. Si votre équipe n'a pas prévu un problème, d'importantes défaillances de production et d'autres problèmes peuvent passer inaperçus.

Observabilité et surveillance : fonctionnement

La différence entre la surveillance et l'observabilité repose sur l'identification des problèmes dont vous savez qu'ils se produiront et sur la possibilité d'anticiper les problèmes qui pourraient survenir. Dans sa forme la plus simple, la surveillance est réactive, tandis que l'observabilité est proactive. Toutes deux utilisent le même type de données de télémétrie, connues comme les trois piliers de l'observabilité.

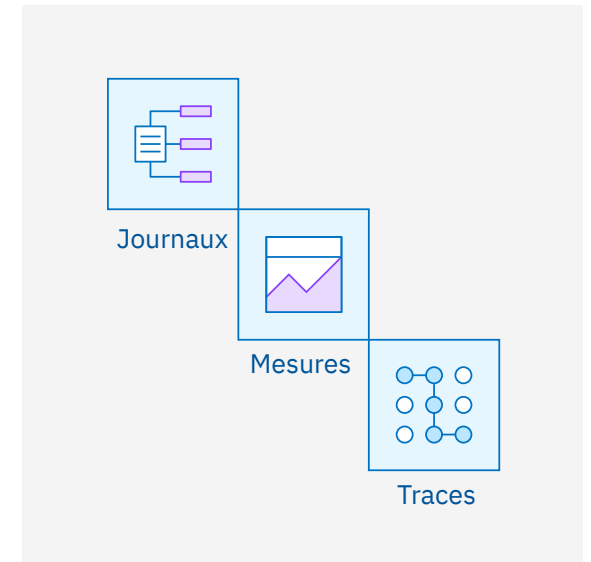
Les trois piliers de l'observabilité sont les suivants :

- **Journaux** : enregistrement de ce qui se passe dans votre logiciel.
- **Mesures** : évaluation numérique des performances de l'application et de l'utilisation des ressources.
- **Traces** : mouvement des opérations dans un système, d'un nœud vers un autre.

Dans le cadre de la surveillance, les équipes utilisent ces données de télémétrie pour définir les mesures en interne et pour créer des tableaux de bord et des notifications préconfigurés. Elles identifient et documentent également les dépendances qui indiquent comment chaque composant d'une application dépend d'autres composants, applications et ressources informatiques.

Une plateforme d'observabilité va encore plus loin dans la surveillance. Les équipes DevOps, les [ingénieurs en fiabilité du site \(SRE\)](#), les équipes d'exploitation et le personnel informatique peuvent établir des corrélations en temps réel entre les données de télémétrie collectées pour obtenir une vue complète de la performance de l'application. Elles comprennent ainsi ce qui compose le système, mais aussi les interdépendances entre les différents composants. La plateforme indique le type d'événement, où il est apparu et la raison pour laquelle il s'est produit, ainsi que les conséquences sur la performance de l'application, guidant ainsi les équipes DevOps dans l'instrumentation de l'application, le débogage et les corrections de la performance.

Les plateformes d'observabilité utilisent également la télémétrie, mais de manière proactive. Elles découvrent automatiquement de nouvelles sources de télémétrie qui pourraient apparaître au sein du système, comme l'appel d'une nouvelle [API](#) vers une autre application logicielle. Pour gérer et collecter rapidement des connaissances exploitables à partir d'un si grand volume de données, la plupart des plateformes disposent de fonctionnalités de [machine learning](#) et d'[AIOps \(intelligence artificielle pour les opérations\)](#) qui permettent de séparer les problèmes réels des problèmes sans rapport.



L'évolution de l'APM vers l'observabilité

Les termes observabilité et [surveillance des performances des applications \(APM\)](#) sont souvent utilisés indifféremment, mais il est plus juste de considérer l'observabilité comme une évolution de l'APM.

L'APM fournit les outils et les processus qui permettent aux services informatiques de déterminer si les applications répondent aux normes de performance et offrent une expérience utilisateur de qualité. D'une manière générale, les outils d'APM surveillent l'infrastructure et portent sur les dépendances d'une application, les transactions métier et l'expérience utilisateur. Ces systèmes de surveillance visent à identifier, isoler et résoudre rapidement les problèmes de performance.

Si l'APM a été la norme pendant plus de deux décennies, du fait de l'essor du développement agile, du DevOps, des [microservices](#), de la multiplicité des langages de production, des

technologies [sans serveur](#) et d'autres technologies [cloud natives](#), il est devenu indispensable pour les équipes de pouvoir surveiller et évaluer plus rapidement des environnements très complexes. Les outils d'APM conçus pour une génération précédente d'infrastructures d'application n'étaient plus en mesure de fournir une visibilité rapide, automatisée et contextualisée sur la santé et la disponibilité de tout un environnement d'application. Aujourd'hui, les nouveaux logiciels sont déployés si rapidement, dans une telle multitude de petits composants, que l'APM parvient difficilement à suivre le rythme.

L'observabilité repose sur les méthodes APM de collecte de données pour répondre plus efficacement à la nature toujours plus accélérée, distribuée et dynamique des déploiements d'applications cloud natives, ce qui facilite la compréhension d'un système et, donc, sa surveillance, sa mise à jour, sa réparation et, finalement, son déploiement.

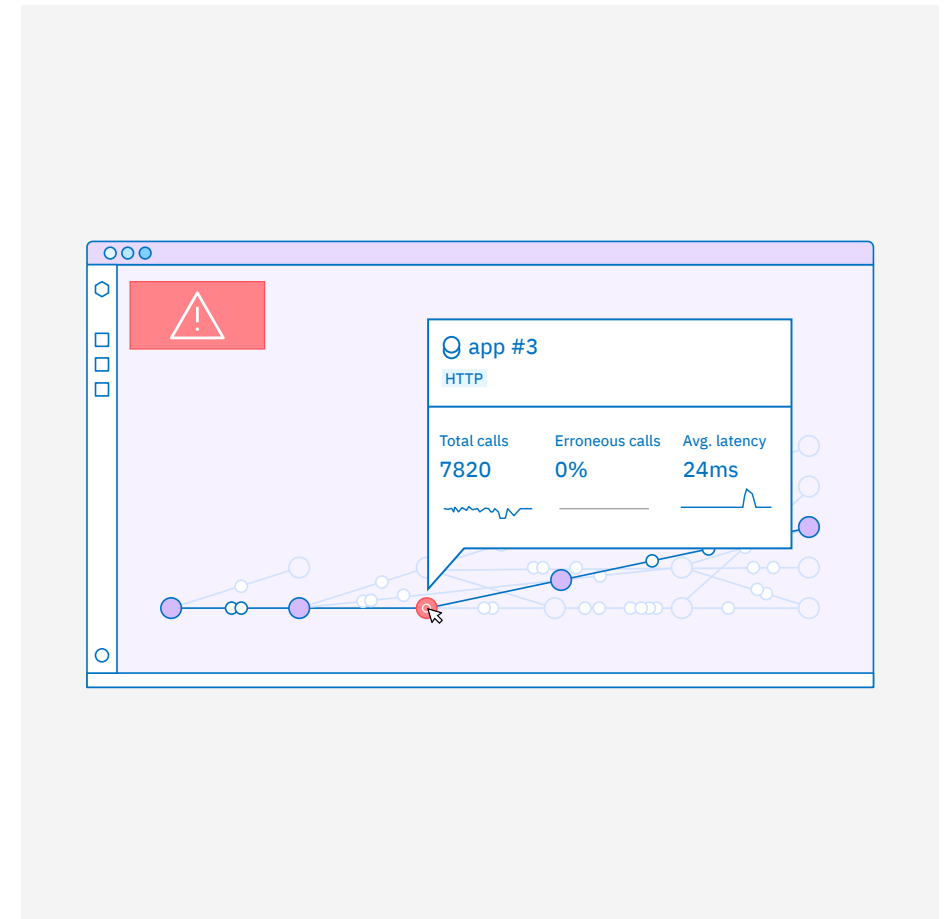
Outils d'observabilité et d'automatisation

Les outils d'observabilité et de surveillance ne se résument pas à la surveillance des états internes et à l'identification et à la résolution des problèmes. Ces plateformes aident les équipes à résoudre les problèmes plus rapidement, ce qui contribue à optimiser les pipelines et permet de consacrer plus de temps aux opérations métier fondamentales et à l'innovation.

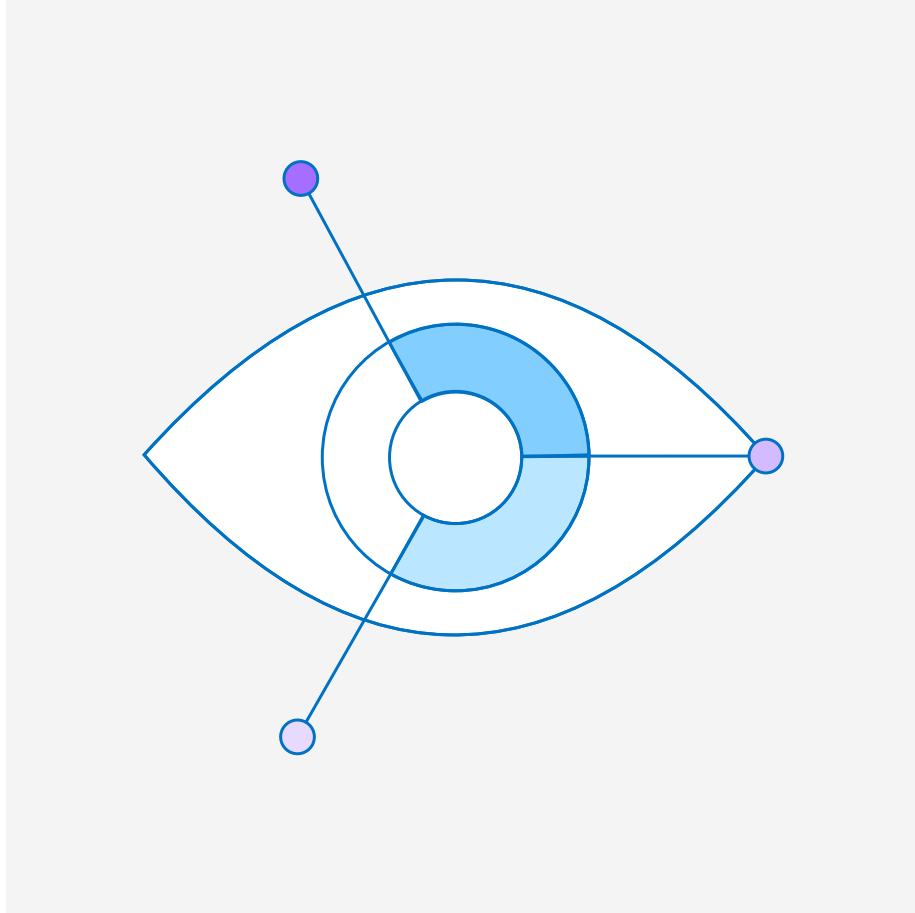
Examinons plus en détail certains types d'outils et d'approches de l'observabilité et de la surveillance :

- **Plateformes d'observabilité** : ces plateformes permettent aux équipes d'intégrer la surveillance, la consignation et le traçage à l'ensemble de l'environnement informatique pour disposer d'une vue complète de l'état du système, même sur des systèmes distribués. Certaines plateformes intègrent également l'expérience utilisateur et le contexte métier afin de fournir une image plus solide de la santé des performances. Selon leur type, ces plateformes fournissent une visualisation des systèmes sur site et des environnements [multiclouds](#) complexes.

- **Code source ouvert** : avec des outils d'observabilité des données à code source ouvert, comme [OpenTelemetry](#), les équipes peuvent surveiller et déboguer les applications, collecter des journaux et des données de mesures, et effectuer un traçage. Ces outils permettent d'exécuter certaines fonctions d'observabilité, mais pas toutes, et il est fréquent que plusieurs soient associés.
- **Automatisation** : l'automatisation de l'observabilité est une simple extension de l'automatisation existante dans le [pipeline CI/CD](#) qui libère plus encore l'équipe DevOps et lui permet ainsi de se consacrer aux tâches principales. Par exemple, [IBM Instana Observability](#) offre des fonctions d'automatisation intelligente de pointe qui améliorent le pipeline CI/CD en automatisant la reconnaissance des applications, de l'infrastructure et des services. Grâce à cette capacité, les développeurs n'ont pas besoin de coder en dur les liaisons des applications et des services après chaque mise à jour. Avec le traitement des incidents optimisé par l'[IA](#), Instana est capable de prévoir les incidents et d'automatiser leur résolution. Un système entièrement automatisé de gestion de la performance des applications surveille chaque service, trace chaque demande et établit le profil de chaque processus.



Observabilité et IBM



Avec Instana, IBM propose une plateforme d'observabilité d'entreprise entièrement automatisée qui fournit le contexte nécessaire pour exécuter des actions intelligentes et optimiser la performance des applications. Par exemple, Instana offre les fonctionnalités et avantages suivants :

- **Automatisation** : bénéficiez d'une observabilité complète dans des environnements dynamiques grâce à la reconnaissance automatique. Vous pourrez tracer chaque demande, enregistrer tous les changements et obtenir des mesures de granularité instantanées.
- **Contexte** : comprenez les interdépendances de toutes les applications pour diagnostiquer les problèmes et en déterminer l'impact. Instana contextualise les données brutes en informations significatives, fournissant ainsi un modèle interactif de relations entre toutes les entités en temps réel.
- **Action intelligente** : détectez et résolvez les problèmes de manière proactive en comprenant les facteurs à leur origine. Analysez chaque demande de l'utilisateur sous tous les angles afin d'identifier et de résoudre rapidement tous les goulots d'étranglement.

Améliorez l'analyse de la performance de vos applications afin d'obtenir le contexte dont vous avez besoin pour résoudre les incidents plus rapidement.



© Copyright IBM Corporation 2023

Compagnie IBM France
17, avenue de l'Europe
92275 Bois-Colombes Cedex

Produit aux USA
Novembre 2022

IBM, le logo IBM et ibm.com sont des marques commerciales d'International Business Machines Corp., inscrites dans de nombreuses juridictions du monde. Les autres noms de services et de produits peuvent être des marques d'IBM ou d'autres sociétés. La liste actualisée de toutes les marques d'IBM est disponible sur la page Web « Copyright and trademark information » à l'adresse www.ibm.com/legal/copytrade.shtml.

Ce document était à jour à la date de sa publication initiale, et peut être modifié sans préavis par IBM. Les offres mentionnées dans le présent document ne sont pas toutes disponibles dans tous les pays où la société IBM est présente.

Les données de performance et les exemples de clients cités sont présentés à titre d'illustration uniquement. Les performances réelles peuvent varier en fonction des configurations et des conditions d'exploitation.

LES INFORMATIONS CONTENUES DANS CE DOCUMENT SONT FOURNIES « EN L'ETAT » SANS AUCUNE GARANTIE, EXPLICITE OU IMPLICITE, Y COMPRIS TOUTE GARANTIE DE QUALITE MARCHANDE, D'ADEQUATION A UN USAGE PARTICULIER ET TOUTE GARANTIE OU EXIGENCE DE NON-CONTREFAÇON. Les produits IBM sont garantis conformément aux dispositions des contrats.