New Relic

White Paper

Conseils pour réduire le délai moyen de résolution (MTTR)

Meilleures pratiques pour une résolution rapide des incidents

Introduction

Le délai moyen de résolution (MTTR) est l'un des indicateurs les plus largement utilisés de la panoplie des outils de fiabilité des systèmes. Paradoxalement, c'est aussi l'un des indicateurs les plus incompris ; nombreux sont les développeurs et les équipes d'exploitation à manquer d'une vision claire sur le MTTR, comme l'utiliser et comment l'améliorer de façon cohérente et durable.

Les organisations modernes dépendent de plus en plus des logiciels pour gérer leur activité. La compréhension inexacte du MTTR n'est pas seulement un inconvénient, elle menace directement les résultats et déstabilise l'expérience client numérique, sans parler des coûts, des risques et de la complexité ajoutés au développement des logiciels.

Quelle solution adopter pour éviter ces problèmes ? Il convient d'appliquer une approche progressive de la définition et de l'application du MTTR, pour associer une instrumentation et une surveillance complète, un processus de réponse aux incidents solide et fiable et une équipe qui comprend comment et pourquoi utiliser le MTTR pour optimiser la disponibilité des applications et leurs performances. Pour vous aider, New Relic a compilé 10 meilleures pratiques pour réduire le MTTR, toutes dans le contexte de mise au point d'une stratégie de réponse aux incidents robuste. Nous allons par ailleurs expliquer comment la plateforme New Relic soutient les objectifs de réduction du MTTR des équipes DevOps de plusieurs façons importantes.

Les différentes interprétations du MTTR

Les défis posés par le MTTR commencent par la définition de ce terme. Son premier sens dans l'ère industrielle concernait la maintenance des machines : le délai moyen de réparation se rapportait au temps nécessaire à la réparation d'une pièce d'une machine, d'un dispositif ou d'un bâtiment.

Dans le monde moderne défini par les logiciels, le MTTR signifie généralement « délai moyen de rétablissement » ou « délai moyen de résolution ».

Même si la distinction paraît insignifiante, ces définitions se rapportent à des résultats différents et reflètent deux approches distinctes de la résolution des problèmes de performance des logiciels :

- Le **délai moyen de rétablissement** est l'équivalent numérique du délai moyen de réparation : temps nécessaire au retour en production d'une application suite à un problème de performance ou une indisponibilité.
- Le **délai moyen de résolution**, d'un autre côté, est plus global : il désigne le temps nécessaire à la résolution d'un problème et l'implémentation de « nettoyages » post-incident ou de mesures proactives pour empêcher une répétition du problème, et déclarer sa clôture.

La deuxième définition du MTTR, plus restrictive, concerne la capacité à identifier et résoudre les causes sous-jacentes des problèmes de performances. Elle évite délibérément les solutions à l'emporte-pièce qui peuvent apporter une solution temporaire à un problème immédiat, mais sans le résoudre pour de bon.

Le MTTR est une statistique, pas une solution miracle

N'oubliez pas que le MTTR est une valeur statistique moyenne. Apprendre à l'utiliser efficacement signifie bien comprendre ses limitations :

Le **MTTR est plus utile comme indicateur prêt à l'emploi lorsque les incidents (et leur résolution) sont de nature similaire.** Si vous avez affaire à des incidents extrêmes dont les temps de résolution sont très variés, le MTTR pris hors contexte risque de vous donner une vue déformée de vos véritables capacités de réponse.

De même, il est facile d'oublier que le MTTR ne prend pas en compte le temps (cela peut paraît surprenant). Le calcul du MTTR ne peut, par exemple, pas capturer la différence essentielle entre les incidents qui impactent vos systèmes et applications pendant les périodes d'utilisation intensive par rapport aux périodes plus calmes.

Aucun de ces aspects ne remet en cause la valeur du MTTR, mais il est important de ne pas oublier l'inconvénient de ne dépendre que d'un seul indicateur.

Deux bonnes pratiques d'utilisation du MTTR peuvent réduire ces risques :

1. **Utilisez le MTTR conjointement à d'autres indicateurs pour comprendre plus précisément et avec plus de nuances les performances de vos applications et de votre infrastructure.** Un bilan d'erreurs est une façon d'y arriver. Il peut montrer, par exemple, qu'une minute de forte activité est équivalente à une heure de trafic faible. Utilisé conjointement au MTTR, un bilan d'erreurs peut vous aider à comprendre le véritable coût et impact de l'indisponibilité et par conséquent comprendre la valeur des pertes et gains dans vos tendances MTTR.
2. **Validez vos efforts de réduction du MTTR en vous concentrant sur la résolution des incidents et en optimisant la disponibilité.** Comme mentionné, résoudre un échec d'application signifie faire toute la lumière sur le problème, trouver le service ou composant d'infrastructure responsable et proposer une solution durable. C'est bien différent d'une solution rapide conçue pour résoudre le problème immédiat, mais sans en comprendre la vraie cause ou ses facteurs déterminants.

Réfléchir en termes de disponibilité contribue à cibler des solutions durables aux problèmes de performances des applications. La disponibilité met l'accent sur la prévention des problèmes récurrents et sur une réflexion portant sur l'impact de ces problèmes sur votre expérience client numérique, même si cette approche implique des solutions plus onéreuses et plus longues à mettre en œuvre qu'une solution à court terme.

Réponse aux incidents : la clé d'une stratégie MTTR gagnante

Une fois que vous avez compris comment utiliser judicieusement le MTTR, la prochaine étape consiste à apprendre comment les équipes DevOps modernes améliorent leurs délais de résolution des incidents et comment elles pérennisent ensuite ces solutions.

En général, les équipes DevOps ont besoin de trois capacités essentielles :

1. Une détection des anomalies proactive, une réponse rapide aux incidents et leur résolution, et des workflows qui accélèrent le processus de correction.
2. Une source unifiée de données multidimensionnelles sur l'état des applications, de l'infrastructure et des performances, formant un contexte sur l'intégralité du système logiciel.
3. Un engagement à améliorer la fiabilité du service à long terme, en augmentant les chances de la pérennité de la résolution des problèmes.

La technologie joue un rôle essentiel pour atteindre ces capacités, mais elle ne peut gagner cette bataille à elle seule. Vous avez besoin d'une stratégie qui associe la technologie, des processus de résolution fiables ainsi que le talent et les compétences de chaque membre de votre équipe.

Votre **processus de réponse aux incidents** doit faire converger tous ces éléments. La réponse aux incidents couvre tous les maillons de la chaîne des événements, en commençant par la détection d'un problème de performances au niveau des applications ou de l'infrastructure, pour se terminer par des connaissances approfondies pour éviter la résurgence du problème. Cela couvre tous les aspects d'une stratégie résiliente pour réduire le MTTR, et garantit que votre équipe peut continuer à s'améliorer, même quand votre activité et vos applications montent en puissance.

Les clés de la création d'un processus de réponse aux incidents d'exception

La discussion sur la réponse aux incidents commence par une question : quelle est la définition d'un incident ? La réponse est essentielle, car le compte à rebours incident-réponse débute au moment de la détection d'un incident.

New Relic définit un incident en tant qu'un problème de performances au niveau d'une application ou de l'infrastructure répondant aux trois critères suivants :

1. **Enjeu élevé pour l'entreprise.** Les incidents impactent les clients, directement ou indirectement.

2. **Urgence.** Les incidents doivent être résolus immédiatement. Pendant un incident, les équipes doivent résoudre un problème dans des délais très courts, en sortant de leur routine quotidienne.
3. **Collaboration.** Les incidents graves nécessitent généralement une collaboration entre plusieurs personnes, travaillant souvent dans différents services de l'entreprise. Coordonner toutes ces personnes pendant une période agitée et sous pression nécessite un type de management particulier et peut induire des coûts imprévus.

Basées sur la manière dont New Relic traite les incidents, ces 10 meilleures pratiques doivent permettre aux équipes de réduire le MTTR en les aidant à améliorer leur stratégie de réponse :

1. Créez un plan d'action rigoureux de gestion des incidents

Au niveau le plus fondamental, les équipes ont besoin d'une politique de remontée des informations claire, qui explique quoi faire en cas de panne : qui appeler, comment expliquer ce qu'il se passe et comment faire avancer la résolution du problème.

La plupart des organisations choisissent une des trois stratégies de gestion des incidents suivantes :

1. **Ad hoc.** Les jeunes entreprises de petite taille choisissent en général cette approche. Lorsqu'un incident se produit, l'équipe détermine qui connaît le mieux la technologie ou le système et affecte la ressource adéquate. Leur structure est légère, c'est tout l'intérêt de cette méthode.
2. **Rigide.** C'est l'approche traditionnelle des équipes de gestion système que l'on trouve dans les entreprises de grande taille, organisées de manière conventionnelle. Le service informatique est généralement chargé de gérer les incidents dans ce type de structure. Les questions de gestion des modifications sont primordiales et les équipes doivent suivre des procédures et des protocoles très stricts. Dans ce cas, la structure n'est pas un obstacle, c'est un avantage.
3. **Fluide.** Il s'agit de l'approche choisie par de nombreuses entreprises modernes, surtout celles qui ont subi des transformations numériques. Les réponses sont adaptées à la nature spécifique des incidents individuels, et elles impliquent une collaboration transversale importante et des compétences pour résoudre les problèmes plus efficacement. Cette approche est basée sur des principes Lean d'expérimentation et d'apprentissage permanents, avec des processus de réponse qui évoluent en permanence dans le temps.

L'approche fluide est celle en général privilégiée par les entreprises de logiciels modernes, à moins d'avoir une raison spécifique pour utiliser le modèle rigide ou ad hoc. Un modèle de réponses aux incidents fluide permet aux entreprises de mobiliser les bonnes ressources et de faire intervenir les collaborateurs possédant les bonnes compétences pour répondre à des situations dans lesquelles il est difficile de faire un diagnostic immédiat, ou de savoir quelles capacités sont requises pour résoudre le problème.

À mesure que les équipes en apprennent plus sur un problème, une approche fluide permet de trouver plus facilement des solutions créatives aux nouveaux problèmes complexes.

2. Définissez des rôles dans votre structure de commandement de la gestion des incidents

Chez New Relic, nous avons nommé un responsable des incidents, qui joue un rôle clé à chaque étape du processus de réponse aux incidents, travaillant comme point central de décision pendant les incidents et aidant les équipes à trouver les meilleurs compromis pendant le processus de réponse. Le responsable des incidents est chargé de diriger les réponses au niveau ingénierie et communication (ce dernier implique de parler avec les clients, à la fois pour collecter

des informations auprès d'eux et les mettre à jour sur l'incident et notre réponse). Le responsable des incidents s'assure que les bonnes personnes sont au courant du problème.

Certaines entreprises nomment des responsables semi-permanents, alors que d'autres établissent une rotation entre plusieurs responsables. Chez New Relic, tous les ingénieurs peuvent tenir ce rôle, car la première personne à réagir à une alerte impactant les clients assume généralement cette fonction.

Chaque incident peut également nécessiter un **chef technique** et un **chef de communication**, chacun reportant au responsable d'incident. Le chef technique, et non le responsable d'incident, énonce la réponse technique spécifique à un incident donné. Dans certains cas, vous pourrez avoir besoin de plusieurs chefs techniques, selon le nombre de systèmes impactés. Le chef technique doit être expert dans le ou les systèmes impliqués dans l'incident, être capable de prendre des décisions informées et d'évaluer les solutions possibles, afin d'accélérer la résolution et optimiser les performances MTTR de l'équipe.

Le chef de communication est le plus souvent choisi parmi le personnel de l'équipe de service client. Cette personne comprend l'impact probable sur les clients et partage ces informations avec le responsable d'incident. En même temps, comme les informations circulent dans la direction opposée, le chef de communication décide de la meilleure façon d'informer les clients des efforts menés pour résoudre l'incident.

3. Formez toute l'équipe aux différents rôles et fonctions

Pour optimiser les avantages d'un modèle fluide, il est logique d'investir dans une formation transversale pour les ingénieurs afin qu'ils puissent assumer plusieurs rôles et fonctions de réponse aux incidents. Il faut toujours des spécialistes de systèmes et technologies spécifiques, mais ne se reposer que sur une poignée d'experts est une invitation au burnout et à la rotation du personnel. Il faut trouver dans les équipes d'autres personnes pouvant acquérir les compétences nécessaires pour résoudre la plupart des problèmes, ce qui permet à vos experts de se concentrer sur les incidents les plus graves et les plus urgents. Des « runbooks » complets (voir Meilleure pratique 7) peuvent constituer une excellente ressource pour réunir et transférer des connaissances techniques spécialisées au sein de votre équipe d'ingénierie.

La formation transversale et le transfert des connaissances vous aident également à éviter l'un des risques les plus dangereux de la réponse aux incidents : nous voulons parler des situations dans lesquelles une personne est la seule dépositaire de la connaissance d'un système ou d'une technologie spécifique. Si cette personne part en vacances ou quitte brusquement la société, les systèmes critiques peuvent se transformer en zones inconnues que personne dans l'équipe ne sait dépanner, par manque de compétences ou de connaissances.

Examinez vos organisations d'ingénierie, évaluez vos dépendances à certaines personnes et mettez en place des référents pour éliminer ces blocages de connaissances, comme vous le faites pour vos ressources système.

4. Surveillez, surveillez, et surveillez encore

C'est une évidence : vous ne pouvez pas réparer des applications ou systèmes si vous ne savez pas qu'ils sont en panne. Une bonne visibilité sur vos applications et votre infrastructure vous permet de mieux réagir en cas d'incidents.

Prenons l'exemple d'un processus de dépannage sans données de surveillance : un serveur hébergeant une base de données critique ou une application tombent en panne, et les seules « données » disponibles pour diagnostiquer le problème sont… le voyant d'alimentation à l'avant du serveur. L'équipe de réponse est obligée de diagnostiquer et résoudre le problème en faisant largement appel à des approximations, ce qui va probablement entraîner un processus de réparation long et coûteux, et certainement un MTTR inacceptable.

Comparez ce scénario avec une situation dans laquelle les données de surveillance en temps réel proviennent de l'application, du serveur et de l'infrastructure associée, communiquant à l'équipe

des chiffres sur la charge du serveur, l'utilisation de la mémoire et du stockage, les temps de réponse et d'autres indicateurs. L'équipe peut formuler une théorie sur la cause du problème et comment le résoudre à l'aide de données tangibles plutôt qu'au hasard.

De plus, les équipes peuvent exploiter les données de surveillance pour évaluer l'impact d'une solution pendant son application, et passer rapidement du diagnostic à la résolution de l'incident. C'est un couple performant, faisant probablement de la surveillance l'outil le plus important pour promouvoir un processus de résolution des incidents efficace et réduire le MTTR.

5. Exploitez les capacités AIOps pour détecter, diagnostiquer et résoudre plus vite les incidents

Un nouvel ensemble de technologies a vu le jour ces dernières années, permettant aux équipes d'astreinte d'exploiter l'IA et le machine learning pour éviter plus d'incidents et y répondre plus vite. Gartner a créé le terme « AIOps » (Artificial Intelligence for IT Operations) pour décrire cette catégorie. AIOps utilise l'IA et le machine learning pour analyser les données générées par les systèmes afin de prédire les problèmes potentiels, déterminer leurs causes profondes et les résoudre de manière automatisée.

AIOps complète vos pratiques de surveillance en fournissant un flux intelligent d'informations sur les incidents s'ajoutant à vos données de télémétrie. En utilisant ces informations pour analyser les données et agir, vous serez mieux préparé pour la détection et la résolution des incidents. Les équipes DevOps et SRE performantes exploitent les capacités AIOps pour répondre rapidement aux incidents et augmenter le temps moyen entre les pannes.

AIOps peut aider dans quatre domaines :

1. **Détection proactive des anomalies** avant qu'un problème arrête la production ou impacte l'expérience client ou les SLO (objectifs de niveau de service).
2. **Réduction du bruit** pour aider les équipes à prioriser les alertes et se concentrer sur des problèmes vitaux, en mettant en corrélation des incidents connexes et en les enrichissant avec des métadonnées et du contexte.
3. **Alerte et remontée intelligentes** pour router automatiquement les incidents vers les personnes ou les équipes les plus compétentes pour agir.
4. **Résolution des incidents automatisée**, avec des workflows pour résoudre les incidents immédiatement et réduire le MTTR.

6. Calibrez avec soin vos outils d'alerte

Avec tous les outils de surveillance disponibles aujourd'hui, on peut se retrouver avec trop d'informations sur les systèmes, ce qui complique la mise au point d'un plan clair pour l'exploitation des données. C'est ici que les alertes programmées deviennent essentielles.

La première étape pratique consiste à configurer des alertes sous forme de seuils d'indicateurs de niveaux de service (SLI). Ce sont des mesures simples, ou seuils, que vous pouvez suivre à l'aide d'outils de surveillance automatisés, et qui indiquent lorsqu'un problème grave risque d'arriver ou est sur le point de se produire. Vous pourriez dire, « si le débit passe en dessous de ce seuil, cela indique un problème dans le système », ou « si les pics de latence dépassent telle durée, nous devons nous en occuper ». Il s'agit de pouvoir quantifier si votre système est robuste.

Par exemple, même si les membres de l'équipe ne connaissent pas tous les détails d'une base de données orientée client, ils peuvent surveiller les seuils et savoir qu'un problème est sur le point de se produire. Quand un système atteint un seuil SLI, il peut envoyer une alerte aux ingénieurs pour qu'ils s'occupent de l'incident potentiel avant que le client n'appelle en panique. Veillez cependant à régler correctement vos seuils d'alerte. Personne n'aime être réveillé à 3 heures du matin pour des problèmes insignifiants.

Choisissez d'autre part un outil d'alerte qui dispose de règles de désactivation, pour vous permettre de garder le contrôle sur les alertes en empêchant les notifications pendant les périodes d'interruption système programmées, par exemple les maintenances périodiques, les déploiements et les tests.

7. Créez des runbooks

Lorsque vous créez des procédures de réponses aux incidents et établissez des pratiques de surveillance et d'alerte, n'oubliez pas de les documenter. Consignez absolument tout et utilisez ces notes pour créer des « runbooks », une documentation qui explique clairement au personnel d'astreinte que faire en cas de problème spécifique.

Utilisez ces runbooks pour recueillir les « connaissances tribales » de votre équipe à propos d'un scénario d'incident-réponse spécifique, dans un seul document. En plus de vous aider à réduire le MTTR, les runbooks sont utiles pour la formation de nouveaux collaborateurs, et particulièrement en cas de départ de membres importants de votre organisation.

Gardez cependant à l'esprit qu'un runbook ne couvrira jamais tous les scénarios. Ce n'est pas un livre de recettes universelles. Il y a tout simplement trop de variables et trop de situations uniques. L'idée est d'utiliser un runbook comme point de départ, pour économiser en temps et en énergie pour traiter les problèmes connus, et permettre à l'équipe de se concentrer sur les aspects les plus complexes et uniques d'un problème.

8. Suivez les incidents pour comprendre comment et pourquoi ils se sont produits

Pour contribuer à réduire le MTTR, vous devez effectuer un suivi de vos incidents, que ce soit par une réunion de résolution, un rapport rétrospectif ou une analyse de fin de projet. Vous allez enquêter sur les événements, essayer de comprendre ce qu'il s'est passé, identifier l'événement déclencheur et ses causes probables et définir des stratégies pour que le problème ne se reproduise pas.

Votre analyse rétrospective ne cherchera pas à pointer du doigt des coupables et vous mettrez en place un processus de non-reproduction des incidents. Dans le cadre de ce processus, tout travail sur un service impliqué dans un incident sera arrêté jusqu'à la résolution du problème ou atténuation de ses causes. Vous renforcerez ainsi l'engagement à résoudre les problèmes plutôt qu'accepter des correctifs à court terme, ce qui aide les équipes à se responsabiliser pour fermer la boucle du processus de résolution des incidents. Ce processus rappelle à tous que la qualité est impérative, et non une option.

9. Entraînez-vous à l'échec avec l'ingénierie du chaos

L'ingénierie du chaos est une technique consistant à introduire de manière aléatoire des problèmes dans vos systèmes, de manière très contrôlée bien sûr, afin de tester sa résilience. L'ingénierie du chaos permet de répondre à des questions cruciales telles que :

- Le système est-il tombé en panne comme vous l'aviez prévu ?
- Avez-vous pu le réparer rapidement ?
- À quoi ressemblaient les données de surveillance ?
- Après combien de temps le service est-il redevenu disponible ?

L'ingénierie du chaos peut profiter à votre organisation de plusieurs façons. D'abord, les équipes apprennent à identifier les moyens de rendre le système plus disponible et plus résilient. Les exercices d'ingénierie du chaos peuvent compléter les répétitions générales de réponse aux incidents, vous permettant de tester vos processus, remontées d'informations, règles, surveillance et alertes, et autres éléments. En éliminant les frictions des situations réelles de réponses aux incidents, ces répétitions peuvent avoir un impact direct sur votre MTTR.

10. Privilégiez le bon correctif, et non le plus rapide

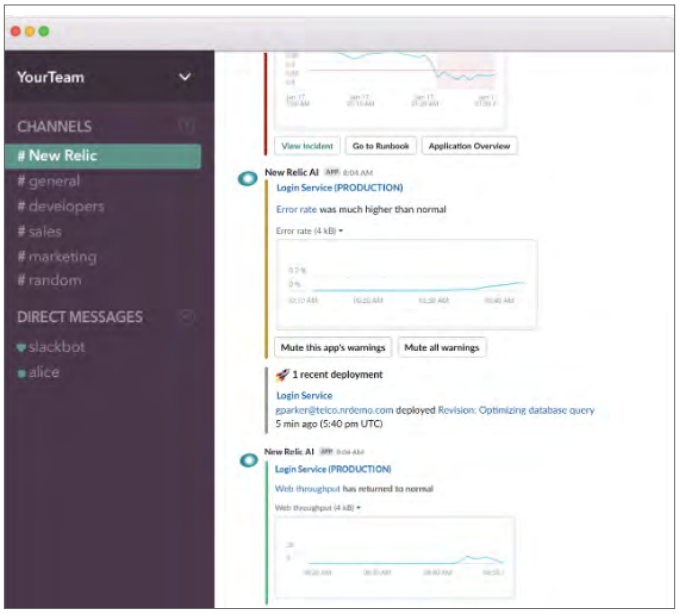
Cela peut s'avérer difficile en pleine tempête, mais essayez de résister aux solutions trop simplistes et en général illusoires. Le MTTR est une moyenne qui comprend tous vos temps de réponse aux incidents. Ce que vous réparez à la va-vite aujourd'hui risque de se retrouver plus tard à l'origine d'un problème qui aurait pu être évité. Occupez-vous des causes sous-jacentes de la baisse des performances sans tarder, vous garantirez ainsi de ne pas revoir le problème vous hanter.

La plateforme New Relic : élevez votre niveau de réponse aux incidents

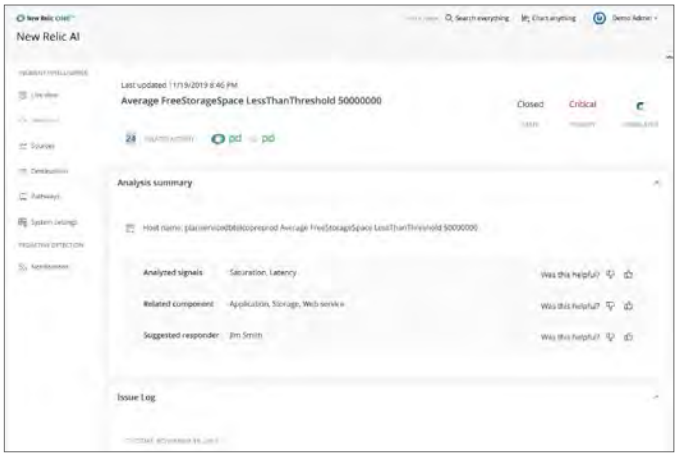
Les 10 meilleures pratiques ci-dessus peuvent vous aider à adopter et intégrer une approche du MTTR basée sur les principes de la réponse aux incidents et de la disponibilité. C'est là que la plateforme d'observabilité de New Relic peut jouer un rôle décisif pour l'adoption de cette approche.

La plateforme New Relic inclut des fonctions de surveillance, d'AIOps, d'alertes, de diagnostic des incidents, ainsi que d'autres fonctionnalités qui contribuent directement à une réponse aux incidents plus rapide, plus intelligente et plus efficace, pour améliorer le MTTR et d'autres indicateurs de performances.

Nos fonctionnalités AIOps complètes, que nous appelons New Relic AI, donnent à votre équipe l'intelligence et l'automatisation pour rechercher, détecter et résoudre les problèmes plus vite. New Relic AI améliore le processus de détection, en faisant remonter à la surface les anomalies concernant plusieurs outils de votre stack et en suggérant des actions pour surveiller des situations similaires à l'avenir. Cerise sur le gâteau, New Relic AI peut utiliser Slack pour vous envoyer des données de panne, pour une évaluation rapide et collaborative des problèmes potentiels.



Mais la détection des incidents n'est qu'un début. New Relic AI exploite les connaissances de référence de l'industrie, puis apprend de vos données et des retours de votre équipe pour éliminer les alertes non pertinentes. New Relic AI met d'autre part en corrélation les incidents connexes, en les enrichissant avec des métadonnées pertinentes et du contexte pour vous aider à diagnostiquer plus vite les problèmes. Vous bénéficiez d'autre part d'un contexte utile sur vos problèmes existants, notamment leur classification en fonction des « quatre signaux forts » (latence, trafic, erreurs et saturation) et des problèmes associés de tout votre environnement. Enfin, New Relic AI peut même vous suggérer quelles sont les personnes de votre équipe les plus à même de traiter un incident spécifique, ce qui vous permettra de réduire le nombre d'alertes inutiles envoyées aux mauvaises personnes.



Des outils qui aident votre équipe à rester alerte, concentrée et efficace

Votre capacité à prévenir les bonnes personnes, rapidement et efficacement, à l'aide de données de performances précises et actionnables, est déterminante pour la réussite de votre stratégie de réponse aux incidents. Les fonctions d'alerte programmées et complètes de New Relic sont à la disposition de votre équipe.

En définissant par exemple des conditions d'alerte reposant sur les résultats de requêtes New Relic Query Language (NRQL) personnalisées, votre équipe peut élaborer des alertes associées à des appels système spécifiques et de charge élevée. Les problèmes de performances sur ces points peuvent fournir des indicateurs identifiant un problème avant qu'il n'impacte des applications de production. Cela laisse à votre équipe le temps de trouver et résoudre des problèmes avant qu'ils ne provoquent des indisponibilités, des pertes de revenus et les plaintes des clients.

Les alertes New Relic contribuent à soulager votre équipe de résolution des incidents dédiée aux environnements de microservices. Des règles d'alerte souples et des options de canaux de notification permettent à votre équipe de mieux contrôler le flux des données d'alerte d'incidents, tout en réduisant le « bruit » provoqué par des conditions d'alerte redondantes.

Des outils qui analysent les performances du système de bout en bout

De plus, les équipes d'exploitation peuvent utiliser New Relic Synthetics pour résoudre un problème crucial qui se pose à de nombreuses équipes DevOps : la surveillance et la compréhension du comportement global du système. Synthetics met à la disposition des organisations une palette d'options pour mesurer les performances des points de terminaison, qu'il s'agisse d'une simple commande ping ou d'une surveillance approfondie qui exécute des scripts simulant des scénarios complexes. Synthetics prend également en charge les agents privés conteneurisés chargés de la surveillance des sites internes et de l'expansion d'une couverture géographique, pour améliorer la sécurité, la préparation au cloud et la souplesse.

Des outils qui vous donnent des informations sur l'expérience utilisateur

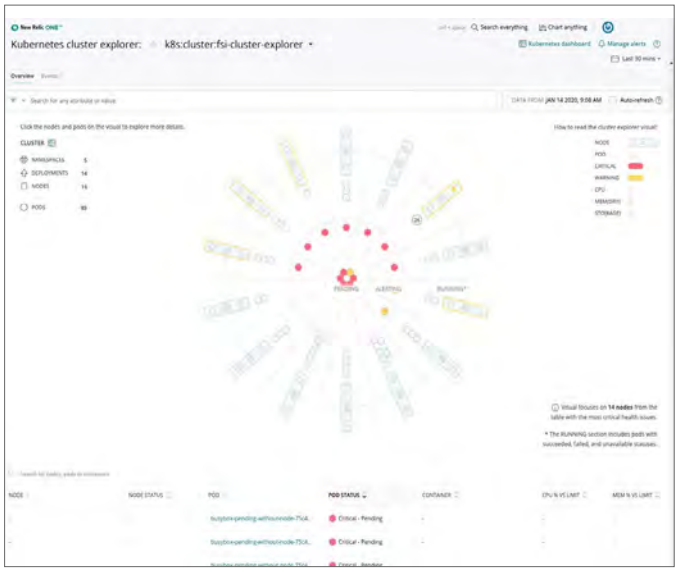
Dans de nombreux cas, une résolution d'incident rapide et réussie passe par la capacité à adopter le point de vue des utilisateurs, qu'il s'agisse de comprendre comment un incident affecte l'expérience client ou d'évaluer l'impact des interactions des utilisateurs. New Relic Browser atteint cet objectif en fournissant une visibilité et des informations complètes sur la façon dont les utilisateurs interagissent avec une application ou un site Web. Browser va au-delà du simple temps de chargement des pages en analysant le cycle de vie complet d'une page, des performances d'une session individuelle et des requêtes AJAX jusqu'aux erreurs JavaScript, en passant par la surveillance des architectures d'applications monopage.

Browser peut de plus vous aider à comprendre l'importance de l'emplacement géographique pendant un incident, en filtrant par exemple les indicateurs de performances et les scores Apdex par région ou pays, et en gérant des listes blanches segmentées par URL et le blocage ou la surveillance spécifique à un domaine.

Des outils pour simplifier le dépannage

Enfin, New Relic aide les organisations à appréhender la complexité croissante des environnements de microservices distribués. La complexité est le prix à payer pour profiter des avantages des microservices, mais elle représente aussi un obstacle majeur à la création d'un processus de résolution des incidents rapide et efficace.

New Relic Kubernetes Cluster Explorer est un bon exemple de comment New Relic aide à donner à votre équipe la clarté et la visibilité sur des systèmes extrêmement complexes, même à très grande échelle. Kubernetes Cluster Explorer fournit une représentation multidimensionnelle d'un cluster Kubernetes qui vous permet de zoomer sur vos espaces de noms, déploiements, nœuds, pods, conteneurs et applications. Cet explorateur de cluster vous permet de récupérer facilement les données et métadonnées de ces éléments, et de comprendre leurs relations à l'aide d'outils de visualisation très intuitifs.



De plus, en passant sans effort de vues globales à des vues très détaillées, Kubernetes Cluster Explorer fournit à toutes les personnes concernées un point de référence unique et partagé pour le dépannage et la compréhension de l'état d'un cluster. Cela peut accélérer votre processus de résolution car tous les intervenants sont tenus au courant simultanément et il n'est pas question de rechercher des « coupables » ni des erreurs de communication.

Les fonctions de traçage distribué de New Relic APM contribuent à réduire la complexité, dans notre cas, les problèmes associés au suivi de la cause de la latence et d'autres problèmes de performances des architectures d'applications distribuées. Le traçage distribué permet à une équipe de suivre le chemin d'une requête lors de son parcours dans un système complexe. Il permet de révéler la latence des composants sur ce parcours et d'en montrer le composant qui crée un blocage.

Le traçage distribué réutilise l'intelligence intégrée à la plateforme New Relic, à l'aide d'outils tels la détection d'anomalies de portée, les graphiques de traces et les demandes personnalisées de données de traces distribuées pour vous aider à isoler, diagnostiquer et résoudre les problèmes rapidement et en toute confiance.

Adopter la bonne approche du MTTR peut s'avérer une tâche complexe ; c'est la réalité de travailler avec des architectures d'applications modernes. Mais avec toutes ces fonctionnalités (et bien d'autres), la plateforme New Relic constitue un outil essentiel pour vous aider à mettre en œuvre un processus de résolution des incidents plus rapide, plus fluide et plus fiable.

Conclusion : gardez à l'esprit la formule de la réussite MTTR à long terme

Enfin, même si le MTTR est important, il ne s'agit pas du seul indicateur pour mesurer la réponse aux incidents. Certes, vous voulez réduire le délai de résolution, mais ne passez pas des centaines d'heures à essayer d'optimiser ce délai et à vous occuper des résultats à court terme.

Mettez plutôt en place des outils comme New Relic qui vous fournit un flux continu d'informations en temps réel, coordonnées avec des règles d'alertes calibrées, puis utilisez ces outils pour soutenir un processus de gestion des incidents résilient. C'est la meilleure formule pour résoudre les incidents de façon systématique et efficace. C'est également la meilleure façon d'améliorer en permanence vos initiatives de réduction du MTTR, avec des gains durable et à long terme en termes de disponibilité des applications.

Créez des logiciels encore meilleurs

Essayez New Relic One sans tarder pour commencer à développer des expériences logicielles de meilleure qualité et plus résilientes. En savoir plus.

New Relic