COLLECTION · CAHIERS COURTS

01

Numéro
de la collection

Du monitoring à l'observabilité

Comprendre le changement de paradigme, et savoir situer son propre système

TERRAOPS

Sommaire

1. Une question que toute organisation finit par se poser 3

2. Ce que la supervision a toujours su faire 4

3. Là où elle s'arrête 5

4. MELT, la matière première de l'observabilité 6

5. Corrélation et haute cardinalité, la vraie puissance 7

6. Construire la matière première, en trois étapes 8

7. De la supervision à l'observabilité, un changement de nature 9

8. Méthode : situer son système en quatre questions 10

9. Les pièges qui guettent une démarche d'observabilité 11

10. Par où commencer : une feuille de route réaliste 11

11. Choisir son outillage sans se tromper 12

12. Dans quelles situations approfondir ce sujet 13

13. Lexique 13

14. Conclusion 15

La méthode, en deux phases 16

1 Une question que toute organisation finit par se poser

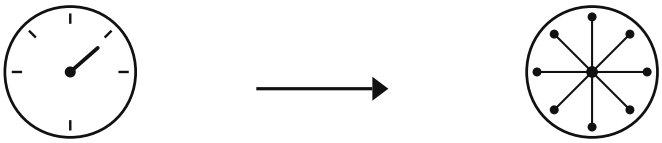
Dans la plupart des entreprises qui exploitent une infrastructure numérique, qu'il s'agisse d'une plateforme e-commerce, d'un système bancaire ou d'un service interne critique, l'incident en production occupe une place particulière dans la vie de l'équipe technique. Il ne se contente pas de coûter du temps d'ingénierie. Il coûte du chiffre d'affaires lorsqu'un service de paiement s'interrompt, il coûte de la confiance lorsqu'un client constate une indisponibilité, et il coûte, plus discrètement mais tout aussi sûrement, de l'énergie humaine, lorsqu'un ingénieur est réveillé à trois heures du matin pour une panne qu'aucun tableau de bord n'avait su anticiper.

Cette réalité s'est aggravée avec la complexification des systèmes. Une application qui reposait il y a dix ans sur quelques serveurs bien identifiés s'appuie aujourd'hui sur des dizaines de microservices, des conteneurs éphémères, des dépendances externes, des couches d'orchestration. Chaque composant supplémentaire est une source de défaillance supplémentaire, et surtout une source de défaillance dont la cause profonde devient de plus en plus difficile à isoler. Les directions techniques le constatent dans leurs propres indicateurs : le nombre d'incidents n'explose pas nécessairement, mais le temps nécessaire pour comprendre chacun d'eux, lui, a tendance à augmenter avec la complexité de l'architecture.

Pour rendre tangible le changement qui traverse aujourd'hui les infrastructures numériques, il est utile de partir d'une image simple.

Imaginez un garage automobile classique. Une voiture entre, un voyant s'allume au tableau de bord. Le mécanicien sait ce que ce voyant signifie, parce que quelqu'un, un jour, a décidé qu'il fallait surveiller cette pièce précise, selon ce seuil précis. Le système fonctionne très bien, tant que la panne appartient à celles que l'on a prévues.

Considérons à présent un stand de Formule 1. Pendant la course, des milliers de capteurs renvoient en temps réel des données sur la température des pneus, la pression hydraulique, les vibrations du châssis ou le comportement du moteur dans chaque virage. Personne n'a programmé un voyant pour chaque panne possible, car cela serait tout simplement impossible : certaines pannes n'ont jamais existé auparavant. Les ingénieurs ne se contentent pas de surveiller des seuils ; ils explorent une télémétrie massive afin de comprendre, en direct, ce qui se passe à l'intérieur du moteur.



Le garage
Un voyant, un seuil

Le stand
Une enquête continue

Du voyant unique à la télémétrie continue

Pendant longtemps, surveiller un système a consisté à configurer des voyants, attendre qu'ils s'allument, puis réagir. Cette approche a fait ses preuves et demeure indispensable. Elle s'arrête néanmoins là où commence l'inattendu, et l'inattendu, dans un système distribué moderne, n'est plus l'exception : il est devenu la norme, et avec lui, le coût associé à chaque heure perdue à en comprendre l'origine.

Ce cahier part d'une question que tout ingénieur SRE ou Ops s'est déjà posée au milieu de la nuit, devant un tableau de bord vert qui ne dit rien d'un système pourtant défaillant : pourquoi est-il cassé ? Nous verrons pourquoi la supervision classique ne peut plus y répondre seule, ce que l'observabilité apporte de véritablement nouveau, et comment situer précisément votre propre infrastructure sur ce chemin. Chaque étape du raisonnement se referme sur un outil directement utilisable : une grille d'audit, une liste de vérifications, une série de questions à poser à votre équipe. Le second cahier de cette collection, « L'observabilité augmentée », prolongera ce parcours en confiant une partie de l'enquête à un agent doté d'intelligence artificielle.

2 Ce que la supervision a toujours su faire

La supervision traditionnelle repose sur un principe simple et, à sa manière, rassurant : on surveille ce que l'on connaît déjà. Une équipe sait quels composants peuvent tomber en panne, un disque qui se remplit, un processus qui consomme trop de mémoire, un service qui cesse de répondre, et configure en conséquence des seuils statiques destinés à les détecter.

Ce mode de fonctionnement répond à une question précise, et une seule : le système fonctionne-t-il ? Il s'agit d'une question binaire, en marche ou à l'arrêt, à laquelle la supervision répond fort bien. Elle se concentre sur l'infrastructure de base, c'est-à-dire la machine, le réseau et les ressources matérielles ou virtuelles : processeur, mémoire, entrées-sorties, disponibilité. Son approche est réactive par construction : on observe des métriques agrégées et l'on agit lorsqu'une alerte franchit un seuil prédéfini.

Il convient de le dire clairement : ce modèle n'est pas dépassé. Il demeure la fondation de toute observabilité sérieuse. Le problème n'est pas qu'il fonctionne mal sur son terrain, bien au contraire. Le problème tient plutôt à l'étroitesse de ce terrain.

Audit express : où en est votre supervision ?

Avant d'aller plus loin, prenez vingt minutes avec votre équipe et listez vos dix alertes les plus fréquentes des trois derniers mois. Pour chacune, notez si le seuil avait été fixé à l'avance, comme un taux d'occupation disque supérieur à 90 %, ou s'il a été ajouté après coup, à la suite d'un incident qui avait échappé à toute règle.

Si la quasi-totalité de vos alertes relève de seuils fixés à l'avance, votre supervision fait très bien son travail, mais elle ne couvre, par définition, que les pannes déjà connues. C'est précisément la limite que la section suivante détaille.

3 Là où elle s'arrête

La supervision classique est conçue pour répondre aux known unknowns, c'est-à-dire aux pannes prévisibles, celles dont on connaît à l'avance la forme, même si l'on ignore le moment où elles surviendront. C'est une force tant que l'incident demeure dans ce périmètre. Dès qu'il en sort, les faiblesses apparaissent, et elles sont structurelles.

La première limite concerne l'investigation. Une alerte de supervision indique généralement qu'un élément est cassé, mais elle n'explique presque jamais pourquoi. En l'absence de contexte détaillé, sans traces ni journaux suffisamment précis, l'équipe constate la panne mais doit reconstruire l'enquête manuellement, souvent dans l'urgence.

La seconde limite est plus insidieuse. On pourrait l'appeler l'effet pastèque : un tableau de bord peut afficher des moyennes globales parfaitement vertes, un temps de réponse moyen correct, un taux d'erreur moyen acceptable, tout en masquant qu'une fraction des utilisateurs vit une expérience catastrophique. Vert en surface, rouge en profondeur. Les moyennes agrégées dissimulent souvent l'essentiel.

La troisième limite est la plus fondamentale. La supervision demeure aveugle aux unknown unknowns, ces événements inédits qu'aucune règle d'alerte n'avait anticipés. Elle ne peut détecter que ce pour quoi une règle a été écrite à l'avance. Un comportement nouveau, une combinaison de facteurs imprévue, un mode de défaillance qui n'existait pas la veille ne déclenchent aucun voyant, simplement parce qu'aucun voyant n'avait été prévu à cet effet.

Repérer un effet pastèque dans vos propres tableaux de bord

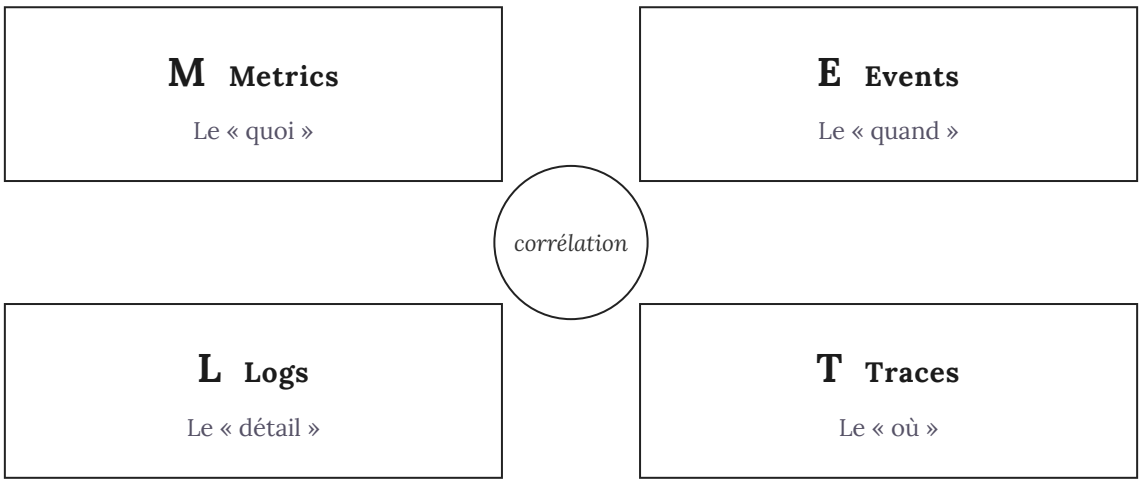
Ne vous fiez jamais à une seule moyenne globale. Croisez systématiquement deux vues : la moyenne d'une part, la distribution d'autre part (percentiles p95 et p99, ou segmentation par cohorte d'utilisateurs, par région, par version de client).

Un signal simple à surveiller : un taux d'erreur moyen inférieur à 1 % peut fort bien dissimuler 15 % d'échecs concentrés sur un segment précis, un pays, un type d'appareil, un palier tarifaire. Si vos métriques ne sont jamais segmentées, vous ne pouvez tout simplement pas voir ce cas de figure, et vos utilisateurs, eux, le vivent.

C'est précisément ce vide que l'observabilité est venue combler.

4 MELT, la matière première de l'observabilité

L'observabilité ne remplace pas la supervision ; elle l'enrichit d'une matière première plus riche, que l'on résume souvent par l'acronyme MELT, pour Metrics, Events, Logs et Traces. Quatre types de signaux, qui répondent chacun à une question différente.



Les quatre signaux MELT et la corrélation qui les relie

Les métriques répondent au « quoi ». Ce sont les données numériques agrégées, celles des tableaux de bord et des alertes globales. Elles prolongent directement la supervision classique : utiles et nécessaires, mais ne racontant qu'une partie de l'histoire.

Les événements répondent au « quand ». Ce sont les points de bascule discrets, comme un déploiement, une modification de configuration ou un changement d'état. Ils constituent souvent la pièce manquante qui permet de relier un symptôme à sa cause, par exemple lorsqu'une erreur commence quelques minutes seulement après un déploiement.

Les journaux, ou logs, répondent au « détail ». Ce sont les enregistrements textuels les plus fins, le grain le plus précis de ce qui s'est réellement produit dans le système. C'est dans ces journaux que se cache, le plus souvent, l'explication concrète d'une erreur.

Les traces répondent au « où ». Elles suivent le parcours d'une requête à travers un système distribué, microservice après microservice, et permettent d'identifier l'endroit exact où se situe un éventuel goulot d'étranglement.

Par où commencer l'instrumentation, concrètement

Si vos quatre signaux sont inégalement couverts, ne cherchez pas à tout traiter de front. L'ordre le plus rentable, constaté sur le terrain, est le suivant : structurez d'abord vos journaux (format JSON, niveaux normalisés, horodatage en UTC), puis propagez un identifiant de corrélation (un identifiant de requête ou de transaction) dans chaque journal, chaque métrique et chaque trace émis.

Cet identifiant commun est le fil qui coud les quatre signaux entre eux. Un standard ouvert comme OpenTelemetry permet aujourd'hui de l'obtenir sans développement spécifique, et évite de lier votre instrumentation à un fournisseur particulier.

5 Corrélation et haute cardinalité, la vraie puissance

Pris séparément, les quatre signaux MELT sont déjà utiles. La véritable puissance de l'observabilité ne vient cependant pas de leur simple accumulation, mais de deux capacités qui permettent de les relier entre eux.

La première est la corrélation, soit la possibilité de naviguer de façon fluide d'une métrique en alerte vers l'événement qui l'a déclenchée, puis de suivre la trace de la requête concernée jusqu'au journal précis qui explique l'erreur. C'est ce parcours continu, plutôt que chaque signal pris isolément, qui transforme une alerte en véritable diagnostic.

La seconde est la haute cardinalité, c'est-à-dire la capacité à filtrer et analyser des données selon des millions d'identifiants uniques, qu'il s'agisse d'un identifiant utilisateur, d'une adresse IP ou d'un identifiant de conteneur. C'est elle qui rend possible l'enquête sur les unknown unknowns, ces problèmes systémiques rares et imprévisibles qui ne se révèlent que lorsqu'on parvient à isoler le bon sous-ensemble de données parmi des millions d'événements.

Repère pour auditer votre propre stack

Pour chacune des quatre lettres de MELT, demandez-vous si la donnée existe, si elle est conservée assez longtemps pour être utile en investigation, et surtout si elle est reliée aux trois autres par un identifiant commun, comme un identifiant de requête ou de transaction.

Une stack qui collecte des métriques, des journaux et des traces dans trois outils qui s'ignorent mutuellement n'est pas encore observable : elle ne fait qu'accumuler de la donnée. La corrélation, pas la collecte, est ce qui fait la différence.

6 Construire la matière première, en trois étapes

La construction de cette matière première suppose trois étapes, qui forment un pipeline continu de la donnée brute jusqu'au diagnostic.

L'instrumentation, d'abord, capture la télémétrie brute (journaux, métriques, traces) par l'intermédiaire d'agents installés au plus près des applications, ou d'interfaces de programmation intégrées au code. C'est l'étape la plus visible, mais paradoxalement la moins différenciante : la plupart des outils modernes la prennent correctement en charge.

L'agrégation et la transformation, ensuite, corrèlent ces données afin de leur donner du contexte et de filtrer le bruit. C'est ici que se joue l'essentiel : un identifiant de corrélation propagé de bout en bout, des étiquettes cohérentes entre les signaux, une normalisation des formats. Une donnée abondante mais incohérente reste une donnée muette.

La visualisation, enfin, permet d'interpréter ces données au moyen de tableaux de bord, pour en dégager les causes racines et les tendances. Elle n'est pas une fin en soi : un tableau de bord n'a de valeur que s'il raccourcit le chemin entre une question et sa réponse.

Point d'attention : la rétention, angle mort des budgets

La question de la durée de conservation est presque toujours sous-estimée. Des journaux conservés sept jours suffisent pour l'exploitation courante, mais rendent impossible l'analyse d'un incident dont les premiers symptômes remontent à trois semaines, un cas beaucoup plus fréquent qu'on ne l'imagine.

Deux règles simples limitent les mauvaises surprises. D'une part, différenciez les durées de rétention par signal : les traces détaillées coûtent cher et peuvent être échantillonnées, tandis que les métriques agrégées se conservent longtemps pour presque rien. D'autre part, surveillez la cardinalité de vos étiquettes : une étiquette mal choisie, comme un identifiant unique placé sur une métrique, peut multiplier les coûts de stockage par cent sans apporter la moindre valeur d'investigation.

7 De la supervision à l'observabilité, un changement de nature

Il existe une manière simple de résumer ce qui sépare ces deux mondes, et elle ne tient pas tant à l'outillage qu'à la nature même de la démarche.

La supervision est un verbe : je surveille mon système. C'est une action posée sur un périmètre défini à l'avance. L'observabilité, à l'inverse, est un nom, une propriété architecturale du système lui-même. Un système est observable ou ne l'est pas, indépendamment de la question qu'on lui pose à un instant donné.

Cette différence de nature en entraîne une autre, relative à la posture. La supervision est réactive, elle alerte sur la panne. L'observabilité est proactive et exploratoire, elle permet d'enquêter sur l'anomalie, même en l'absence d'alerte déclenchée.

Elle en entraîne enfin une troisième, relative à la cible. La supervision couvre les known unknowns, c'est-à-dire les pannes prévisibles, tandis que l'observabilité ouvre la voie aux unknown unknowns, les événements inédits.

	Supervision	Observabilité
Nature	Un verbe (surveiller)	Un nom (une propriété)
Posture	Réactive	Proactive, exploratoire
Cible	Known unknowns	Unknown unknowns
Question	Est-il cassé ?	Pourquoi est-il cassé ?

Quatre différences de nature, une même bascule

Tout se résume, au fond, à une question qui change de nature. La supervision demande si le système est cassé. L'observabilité demande pourquoi il est cassé.

8 Méthode : situer son système en quatre questions

Cette distinction n'a d'intérêt que si elle permet de juger où en est réellement votre infrastructure. Posez-lui, dans l'ordre, les quatre questions suivantes.

1. Nature. Quand un incident survient, votre équipe consulte-t-elle un système déjà interrogeable de toutes parts, ou bien lance-t-elle dans l'instant une action de surveillance ad hoc, un script, une commande, une connexion manuelle ? Dans le premier cas, vous tenez une propriété du système. Dans le second, vous tenez une action humaine répétée à chaque incident.

2. Posture. Vos investigations démarrent-elles uniquement après qu'une alerte a franchi un seuil, ou vous arrive-t-il d'explorer un comportement simplement parce qu'il paraît inhabituel, sans qu'aucune règle ne l'ait signalé ? La seconde capacité ne s'achète pas avec un outil : elle se construit avec des données suffisamment riches pour être explorées librement.

3. Cible. Listez vos cinq derniers incidents significatifs. Combien correspondaient à une panne déjà anticipée, avec un seuil ou une règle prête à l'avance ? Combien étaient réellement inédits ? Plus la seconde catégorie pèse lourd, plus votre besoin d'observabilité véritable, par opposition à la simple supervision, est avéré.

4. Temps de réponse. Chronométrez, sur votre dernier incident, le délai entre l'alerte et la compréhension réelle de sa cause. Si ce délai se mesure en minutes, votre système est observable. S'il se mesure en heures, vous disposez d'une bonne supervision, mais pas encore d'une véritable observabilité.

Cette grille n'a pas vocation à classer une infrastructure dans une case définitive, mais à révéler, question après question, où porter l'effort en priorité.

> **Piège fréquent : brûler les étapes**
>
> Ne sautez pas cette phase pour vous lancer directement dans un outillage plus sophistiqué (plateformes avancées, et à plus forte raison agents dotés d'intelligence artificielle, sujet du second cahier de cette collection). Investir dans la couche supérieure avant d'avoir répondu correctement à ces quatre questions revient à équiper un stand de Formule 1 avec les capteurs d'un garage de quartier : la promesse technologique ne compense jamais un déficit de matière à interroger.

9 Les pièges qui guettent une démarche d'observabilité

Les organisations qui échouent dans leur transition vers l'observabilité échouent rarement par manque d'outils. Elles échouent sur quatre écueils récurrents, qu'il est plus économique de connaître à l'avance que de découvrir en production.

Le premier est le silo d'outils. Une console pour les métriques, une autre pour les journaux, une troisième pour les traces : chaque outil est excellent, mais l'enquête impose de copier des horodatages d'un écran à l'autre, en espérant que les horloges concordent. La donnée existe, la corrélation n'existe pas, et c'est elle qui fait l'observabilité.

Le deuxième est l'explosion silencieuse des coûts. La haute cardinalité est une capacité précieuse, mais elle se paie : chaque étiquette supplémentaire multiplie les séries à stocker. Une équipe qui instrumente sans gouvernance découvre généralement le problème sur sa facture, plusieurs mois plus tard.

Le troisième est la fatigue d'alerte. Multiplier les signaux sans discipline conduit à un bruit de fond permanent, que les équipes apprennent à ignorer, y compris le jour où l'alerte est réelle. Une alerte qui ne déclenche aucune action documentée n'est pas une protection : c'est une nuisance.

Le quatrième, enfin, est le tableau de bord musée : de superbes visualisations construites après chaque incident, que plus personne ne consulte trois semaines plus tard. Un tableau de bord n'a de valeur que s'il répond à une question que l'équipe se pose encore.

Règles d'hygiène pour un système d'alerte qui reste crédible

Chaque alerte doit être actionnable : si personne ne sait quoi faire lorsqu'elle se déclenche, elle doit être supprimée ou transformée en simple signal d'information. Passez en revue, chaque trimestre, les alertes qui n'ont jamais conduit à une action : c'est votre gisement de bruit.

Alertez sur les symptômes vécus par l'utilisateur (latence, taux d'erreur, disponibilité d'un parcours critique) plutôt que sur les causes internes supposées. Un processeur à 95 % n'est pas un incident si personne ne s'en aperçoit ; un parcours de paiement dégradé en est un, quelle que soit la charge processeur.

10 Par où commencer : une feuille de route réaliste

La transition vers l'observabilité n'exige ni big bang ni refonte d'outillage. L'expérience montre qu'un chemin progressif, sur un trimestre, suffit à changer concrètement la manière dont une équipe vit ses incidents.

Le premier temps consiste à choisir un périmètre restreint mais réel : un service critique, un parcours utilisateur important, plutôt que l'ensemble du système. Sur ce périmètre, structurez les journaux et propagez un identifiant de corrélation de bout en bout. C'est un travail modeste, dont l'effet se fait sentir dès la première investigation.

Le deuxième temps ajoute les traces distribuées sur ce même périmètre, et relie les trois signaux dans une interface commune. À ce stade, l'équipe doit pouvoir dérouler le parcours complet (métrique, événement, trace, journal) sans changer d'outil ni copier un horodatage à la main.

Le troisième temps consolide la discipline : revue des alertes existantes à la lumière des règles d'hygiène de la section précédente, définition des durées de rétention par signal, et mesure systématique du délai entre alerte et compréhension de la cause, incident après incident. C'est cet indicateur, plus que tout autre, qui dira si votre observabilité progresse réellement.

Astuce : faire de chaque incident un investissement

Instaurez une règle simple : chaque analyse post-incident doit se conclure par au moins une amélioration d'observabilité : un journal enrichi, une étiquette ajoutée, un lien de corrélation créé. Un incident dont on ne tire qu'un correctif répare le passé ; un incident dont on tire aussi de l'instrumentation prépare l'enquête suivante.

11 Choisir son outillage sans se tromper

Le marché de l'observabilité est abondant, et les critères mis en avant par les éditeurs (richesse des visualisations, nombre d'intégrations, tarification à l'ingestion) ne sont pas toujours ceux qui comptent en investigation réelle. Trois critères, dans l'ordre, méritent de guider le choix.

Le premier est la capacité de corrélation native : depuis une métrique en alerte, combien de clics faut-il pour atteindre la trace, puis le journal correspondant ? Si la réponse suppose de changer d'outil ou de recopier un horodatage, le reste importe peu. Exigez une démonstration sur ce parcours précis, avec vos propres données si possible.

Le deuxième est le comportement face à la cardinalité : que se passe-t-il, techniquement et financièrement, lorsque vos données comportent des millions d'identifiants uniques ? Certains outils dégradent leurs performances, d'autres dégradent votre budget. Les deux se découvrent rarement pendant la phase d'essai.

Le troisième est la réversibilité : une instrumentation fondée sur un standard ouvert comme OpenTelemetry se transporte d'un outil à l'autre ; une instrumentation propriétaire

vous lie à son éditeur pour des années. Le coût de sortie fait partie du coût total, même s'il n'apparaît sur aucun devis.

> **Astuce : le test des trois incidents**
>
> Avant de retenir un outil, rejouez-y vos trois derniers incidents significatifs, à partir de vos données réelles. Mesurez le temps nécessaire pour reconstituer chaque enquête, de l'alerte initiale au journal explicatif. C'est un protocole d'évaluation plus fiable que n'importe quelle grille de fonctionnalités : il teste l'outil sur votre réalité, pas sur la démonstration de l'éditeur.

12 Dans quelles situations approfondir ce sujet

Toutes les organisations n'ont pas le même degré d'urgence à investir dans l'observabilité. Le sujet devient prioritaire lorsque plusieurs conditions se cumulent : une architecture distribuée, où la cause d'un incident traverse plusieurs services ; des incidents dont une part croissante est réellement inédite, sans règle d'alerte préexistante ; un temps de diagnostic qui se mesure en heures plutôt qu'en minutes ; et une équipe dont l'énergie s'épuise en reconstructions manuelles d'enquêtes.

À l'inverse, un système simple, stable, aux modes de défaillance bien connus, peut légitimement s'en tenir à une supervision rigoureuse. L'observabilité est une réponse à la complexité ; elle n'est pas une fin en soi.

13 Lexique

Les termes qui suivent reviennent dans toute conversation sur l'observabilité. En donner une définition partagée au sein de l'équipe évite bien des malentendus.

Cardinalité.
Nombre de valeurs distinctes que peut prendre une étiquette : un identifiant utilisateur est de haute cardinalité, un nom d'environnement de faible cardinalité. La haute cardinalité rend l'enquête possible, et coûteuse.

Corrélation.
Capacité à relier les quatre signaux MELT entre eux par un identifiant commun, pour parcourir sans rupture le chemin de l'alerte au journal explicatif.

Échantillonnage.

Conservation d'une fraction seulement des traces afin d'en maîtriser le coût, au prix d'une visibilité partielle. À réserver aux signaux volumineux, jamais aux événements rares que l'on cherche justement à retrouver.

Effet pastèque.
Tableau de bord vert en surface, expérience utilisateur rouge en profondeur : les moyennes agrégées masquent la souffrance d'un segment.

Événements (Events).
Points de bascule discrets répondant au « quand » : déploiement, changement de configuration, modification d'état. Souvent la pièce qui relie un symptôme à sa cause.

Instrumentation.
Travail consistant à faire émettre au système sa télémétrie, par des agents ou des bibliothèques intégrées au code. Étape la plus visible, mais la moins différenciante.

Journaux (logs).
Enregistrements textuels fins répondant au « détail » : la trace écrite, au grain le plus précis, de ce qui s'est réellement produit dans le système.

Known unknowns.
Pannes prévisibles : on en connaît la forme à l'avance, même si l'on ignore quand elles surviendront. Terrain naturel de la supervision.

MELT.
Acronyme des quatre signaux de l'observabilité : Metrics (métriques), Events (événements), Logs (journaux) et Traces. Leur valeur vient de leur mise en relation, pas de leur simple accumulation.

Métriques (Metrics).
Données numériques agrégées répondant au « quoi » : temps de réponse, taux d'erreur, charge. Support des tableaux de bord et des alertes globales.

MTTR.
Temps moyen de résolution d'un incident. L'indicateur le plus lisible des progrès d'une démarche d'observabilité, à condition de mesurer aussi le temps de compréhension, qui en est la composante la plus compressible.

Observabilité.
Propriété d'un système qui permet de comprendre son état interne à partir des signaux qu'il émet, y compris pour des questions qu'on n'avait pas prévues. À distinguer de la supervision, qui ne répond qu'aux pannes anticipées.

OpenTelemetry.

Standard ouvert d'instrumentation qui rend la télémétrie portable d'un outil à l'autre et évite de dépendre d'un seul éditeur.

Percentiles (p95, p99).
Valeurs sous lesquelles se situent 95 % ou 99 % des mesures. Ils révèlent l'expérience des utilisateurs les moins bien servis, là où la moyenne la dissimule.

Rétention.
Durée de conservation des signaux. Trop courte, elle interdit l'analyse d'un incident ancien ; uniforme, elle coûte cher inutilement.

SRE / Ops.
Ingénierie de la fiabilité (Site Reliability Engineering) et exploitation : les équipes chargées de tenir un système en production.

Supervision (monitoring).
Surveillance de composants connus au moyen de seuils fixés à l'avance. Répond à la question « le système fonctionne-t-il ? ». Fondation nécessaire de l'observabilité, mais aveugle à l'inattendu.

Télémétrie.
Ensemble des données brutes émises par un système (journaux, métriques, traces) et collectées à distance pour être analysées.

Traces.
Suivi du parcours d'une requête à travers un système distribué, répondant au « où » : quel service, quel maillon ralentit.

Unknown unknowns.
Événements inédits, qu'aucune règle d'alerte n'avait anticipés. Terrain propre de l'observabilité.

14 Conclusion

Nous sommes partis d'une question posée au milieu de la nuit, devant un tableau de bord vert qui ne disait rien d'un système pourtant défaillant : pourquoi est-il cassé ? La supervision classique ne peut y répondre que pour les pannes qu'elle a anticipées. L'observabilité, construite sur les métriques, les événements, les journaux et les traces, reliés par la corrélation et la haute cardinalité, ouvre la voie à l'enquête sur l'inattendu.

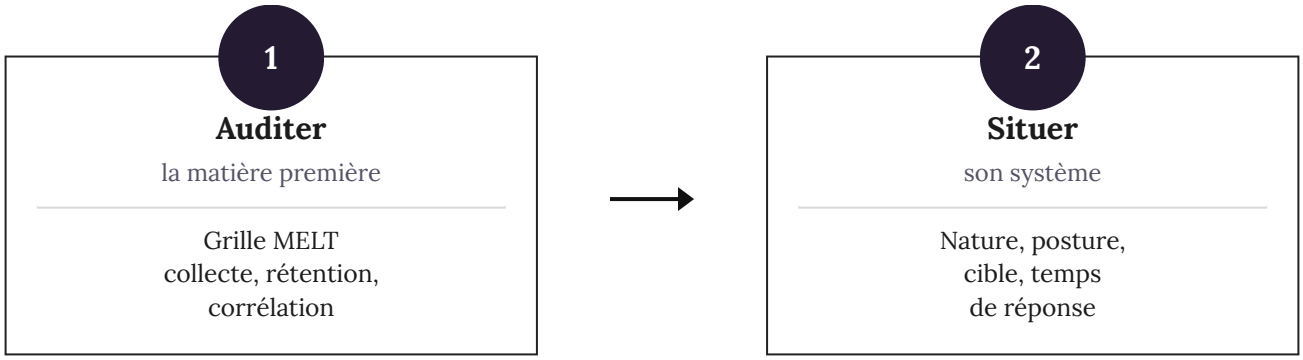
Ce basculement n'est pas d'abord une affaire d'outils. C'est un changement de nature (d'un verbe vers un nom, d'une posture réactive vers une posture exploratoire, d'un périmètre prévu vers un territoire inconnu) qui se construit méthodiquement : une matière première

auditée, un système situé avec lucidité, une discipline d'alerte et de rétention tenue dans la durée.

Reste une question, que ce cahier a volontairement laissée ouverte : une fois la matière disponible, qui l'explore, en continu ? L'attention humaine ne s'étend pas à volonté, et les tableaux de bord les plus riches demeurent passifs tant que personne ne les interroge. C'est précisément l'objet du second cahier de cette collection, « L'observabilité augmentée » : confier le premier niveau de cette enquête à un agent doté d'intelligence artificielle, et examiner, cas réel à l'appui, ce que cela exige véritablement.

La méthode, en deux phases

Ce cahier a disséminé, au fil de ses sections, les outils d'un diagnostic complet. Rassemblés ici dans l'ordre où ils doivent être employés, ils forment un protocole reproductible, applicable à n'importe quelle infrastructure, indépendamment du secteur d'activité ou de la taille de l'équipe.



Auditer, puis situer : les deux phases de ce cahier

Phase 1 : auditer la matière première

Reprenez la grille MELT présentée à la section 5. Pour chacun des quatre signaux, métriques, événements, journaux, traces, vérifiez trois points : la donnée est-elle collectée, est-elle conservée assez longtemps pour servir une investigation a posteriori, et surtout, peut-elle être reliée aux trois autres signaux par un identifiant commun. Une organisation qui ne peut répondre positivement à cette dernière question, quelle que soit la sophistication de ses outils, n'est pas encore observable au sens propre. Elle accumule de la donnée plutôt qu'elle ne la corrèle.

Phase 2 : situer son système sur l'échelle supervision-observabilité

Appliquez ensuite la grille en quatre questions détaillée à la section 8 : nature, posture, cible et temps de réponse. Cette phase a un objectif précis : déterminer où concentrer l'effort, entre consolidation des fondations et exploration de capacités nouvelles ; et, le

moment venu, juger si votre organisation est prête pour la troisième phase, la sécurisation d'un agent qui enquête, détaillée dans le second cahier de cette collection.

Fiche de synthèse, à afficher près de l'écran d'astreinte

- La grille MELT a été passée en revue : collecte, rétention, corrélation, pour chacun des quatre signaux.
- Un identifiant de corrélation relie effectivement métriques, journaux et traces sur au moins un parcours critique.
- Les tableaux de bord croisent moyennes et distributions (p95, p99) sur les parcours utilisateurs essentiels.
- Les quatre questions (nature, posture, cible, temps de réponse) ont été posées en équipe, et les réponses notées.
- Le délai entre alerte et compréhension de la cause est chronométré à chaque incident, et suivi dans le temps.

Contributions

Ce cahier s'appuie sur les sessions de partage animées par Moustafa Bendjema, Techlead chez TerraOps, consacrées au passage du monitoring traditionnel à l'observabilité, et sur les retours d'expérience recueillis auprès des équipes Ops accompagnées. Collection imaginée et dirigée par Pascale Ah-Toy.

Cahier TerraOps · Collection éditoriale

Numéro 1 · 1er septembre 2026

COLLECTION CAHIERS COURTS · NUMÉRO 01

Un tableau de bord vert qui ne dit rien d'un système pourtant défaillant : tout ingénieur SRE ou Ops connaît cette scène. Ce cahier raconte comment passer du *garage* au *stand de Formule 1*, de la supervision qui surveille des seuils à l'observabilité qui permet d'enquêter.

Il détaille la matière première de l'observabilité (métriques, événements, journaux, traces), les deux capacités qui la rendent réellement puissante, et les pièges les plus fréquents d'une démarche d'observabilité.

Une méthode reproductible referme ce cahier : une grille d'audit MELT, quatre questions pour situer son système, et une feuille de route pour progresser.

TERRA OPS

contact@terraops.fr · www.terraops.fr