AIOps - Mythe ou Réalité ?

Jérôme Durand
Cisco Systems
11 rue Camille Desmoulins
92 782 Issy-les-Moulineaux Cedex 9

Résumé

AIOps (AI - Artificial Intelligence) semble être le dernier terme à la mode dans le monde des systèmes et réseaux. Derrière toute l'agitation du marché et les délires des équipes marketing de nombreux constructeurs, l'application des principes de l'intelligence artificielle à l'opération de réseaux informatiques est bel et bien une réalité. Les usages de l'intelligence artificielle se développent dans tous les domaines et les réseaux ne font pas exception.

On distinguera deux grands groupes quand on parle d'intelligence artificielle : le Machine Learning qui apprend et permet d'établir des modèles à partir de données, et le Machine Reasoning qui permet d'automatiser l'application d'un modèle préalablement établi. Ces deux familles d'algorithmes promettent de remonter des informations plus pertinentes quant au fonctionnement des réseaux et systèmes en n'indiquant que des informations utiles globales et non des métriques individuelles.

Mais derrière toutes ces promesses se cache une réalité : AIOps n'est pas à la portée de tout le monde tant l'investissement requis est monumental (temps, moyens…), avec au final peu de réussite. Seuls les acteurs qui possèdent suffisamment de données pourront tirer leur épingle du jeu. Pour l'utilisateur final, il s'agira de déployer un produit qui utilise ces principes en se focalisant avant tout sur les bénéfices.

Mots-clefs

AIOps, Machine Learning, Machine Reasoning, Predictive Internet, Deep Learning, ontologie, supervision.

1 Qu'est-ce que l'AIOps ?

1.1 Définition

L'AIOps est l'application de l'intelligence artificielle pour l'opération des technologies de l'information (informatique, réseau…) Le terme MLOps (*Machine Learning*) est aussi utilisé mais comme nous le verrons plus tard, cette dernière dénomination est réductrice.

1.2 Pourquoi l'AIOps ?

Les infrastructures informatiques ont considérablement évolué au cours des dernières décennies. Accroissement du nombre de terminaux et des usages, la mobilité, l'avènement du cloud, la containerisation et les micro-services, la professionnalisation des attaques informatiques, etc. Ce sont autant d'exemples qui montrent que les infrastructures se sont énormément complexifiées et diversifiées, posant un réel challenge sur les équipes opérationnelles. Observer des indicateurs relevés de-ci de-là ne suffit plus à garantir le bon fonctionnement du réseau et de ses applications.

1.3 Pet or Cattle ?

Animal de compagnie ou bétail ? Tous les systèmes ne s'opèrent pas de la même manière… Le nombre d'équipements sous la responsabilité des équipes IT a été décuplé. S'il était autrefois possible de choyer chaque système avec une supervision adaptée, il convient aujourd'hui d'adopter d'autres méthodes pour faire face à la quantité d'informations remontées. Prenons l'exemple d'une application critique qui tournait autrefois nativement sur un serveur bien identifié par l'administrateur. Cette dernière peut maintenant être décomposée en micro-services, tournant sur une ferme de serveurs, et même parfois sur des supports hybrides (*datacenter* local, *cloud*…) Si les gains sont immenses pour les équipes de développement qui gagnent en agilité, le challenge est énorme pour les équipes opérationnelles. Et paradoxalement, l'application doit intégrer nativement tous les mécanismes pour faire face à la perte d'une composante. Il devient très compliqué d'opérer l'application, car son comportement est partiellement déconnecté des supports utilisés et traditionnellement supervisés. C'est tout le paradigme que l'on adresse avec des approches DevOps. On va regrouper les équipes opérationnelles et de développement pour gagner en cohérence et intégrer la gestion de l'application très tôt dans les processus de développement. L'AIOps peut se révéler très pertinente pour la supervision et les opérations de tels systèmes : plutôt que de relever chaque métrique, chaque état de tous les sous-systèmes et d'appliquer des seuils unitaires, on va laisser l'algorithme remonter des anomalies plus globales.

1.4 Maîtriser de bout en bout

Une autre problématique est que l'infrastructure informatique est de plus en plus éparse avec des éléments qui ne sont pas parfaitement sous contrôle. La mobilité des terminaux et le cloud sont deux exemples qui illustrent cette complexité. Qui peut se targuer de maîtriser la qualité de connexion sur des supports comme le Wi-Fi, la 5G ou l'internet ? Les opérations des services dépendent d'éléments qui sont en dehors de notre contrôle et pour lesquels on dispose d'informations limitées, provenant de sources distinctes. C'est aussi pour ces problématiques globales qu'un management traditionnel atteint rapidement ses limites : le nombre de supports explose et il convient d'agréger des données éparses dans un *data lake* puis d'automatiser leur analyse.

1.5 Au-delà de la technique, les impacts pour les métiers

On note une grande appétence pour l'AIOps par les métiers. Devant la complexité des infrastructures, ce sont avant tout les métiers, consommateurs d'informatique, qui ont le plus besoin de fiabiliser les opérations, et détecter l'indécelable pour garantir le meilleur fonctionnement de leurs applicatifs. Les métiers investissent donc très largement dans l'intelligence artificielle en espérant bénéficier de gains immédiats.

1.6 De la nécessité de faire des recherches avant de se lancer…

Malheureusement, selon une étude du cabinet l'analyste Gartner [1], seuls 15 % des projets d'intelligence artificielle sont déployés en production et le temps de mise en œuvre d'un simple pilote dure entre 12 et 18 mois en moyenne. Il faut d'emblée se rendre à l'évidence : l'intelligence artificielle est un sujet compliqué, coûteux et qui ne peut pas tout. C'est la raison pour laquelle il convient de dépasser l'effet de mode et de se pencher plus sérieusement sur l'AIOps.

2 L’intelligence artificielle

L’intelligence artificielle est une dénomination souvent choyée par les équipes *marketing* qui va regrouper plusieurs approches techniques dont les principales sont mentionnées ci-après [2].

2.1 Machine Learning

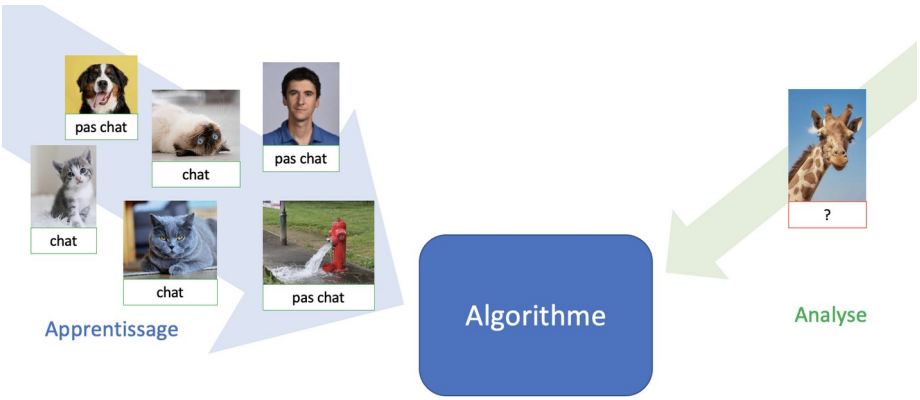
On va laisser l’algorithme apprendre de lui-même et catégoriser les données source. Il déterminera, par exemple, ce qui est un comportement normal et remontera les anomalies ou toute autre information utile qu’il détectera après une période d’apprentissage. L’objectif est, avant tout, de déterminer un modèle qui pourra s’appliquer dans un environnement donné. L’enjeu principal est d’aider l’algorithme dans son apprentissage pour qu’il puisse s’affiner et présenter des résultats cohérents. Supposez que vous avez généralement 10 Mbit/s de trafic sur un lien et que celui-ci passe à 20 Mbit/s. Est-ce que cette augmentation considérable de 100 % de débit est une anomalie ? Il ne s'agit, après tout, que de 10 Mbit/s en plus… C’est l’apprentissage qui va permettre de faire le tri.

2.1.1 Apprentissage

L’apprentissage est ce qui va permettre d’éduquer l’algorithme et prendre les bonnes décisions. Comme nous le verrons plus tard, c’est vraiment l’apprentissage et les données utilisées qui vont permettre de distinguer les solutions entre elles. Il en existe plusieurs formes dont les principales sont listées ci-après.

Apprentissage supervisé

L’idée consiste à injecter des données dans le système avec un résultat connu. L’algorithme va apprendre à partir de ces informations les corrélations entre les données et les résultats, et va pouvoir appliquer le modèle trouvé sur toute nouvelle entrée à venir. Pour reprendre l’exemple précédent, il faudrait alors qu’un administrateur puisse injecter dans le système toutes les augmentations soudaines de trafic des dernières années et indiquer pour chacune d’entre elles si cela relève d’une anomalie ou non. L’algorithme apprendra alors à distinguer le bon grain de l’ivraie et pourra appliquer les principes sur les futures données.



Apprentissage supervisé

En pratique, ce type d’apprentissage n’est pas toujours adapté à l’AIOps pour deux raisons principales :

– les équipes IT n'ont pas la capacité matérielle (temps/moyens) de faire ce travail de dichotomie. Elles recherchent des outils clé en main qui ont éventuellement bénéficié d'un apprentissage réalisé par des concepteurs de logiciels, et qui de fait doivent rester génériques ;

– il n'est pas possible de caractériser une anomalie à partir d'une seule dimension (l'augmentation de débit). Il y a, en pratique, bien d'autres paramètres qui vont intervenir (type de trafic, type de lien, QoS configurée, matériel déployé…). Il existe trop de variables et de spécificités qui vont rendre cette approche difficile à utiliser en pratique.

Apprentissage non-supervisé

A contrario, dans ce cas-présent, l'algorithme ne part de rien. Il apprend de lui-même à partir des données qu'il reçoit au fur et à mesure. Il est intéressant pour l'AIOps, car il est particulièrement adapté dans des environnements multidimensionnels dans lesquels de nombreuses raisons peuvent être la source de problèmes. L'algorithme va pouvoir faire des recoupements entre les données et remonter les corrélations découvertes.

Pour revenir à l'exemple précédent, il décidera donc tout seul du caractère anormal ou non de l'augmentation de trafic de 10 Mbit/s par rapport à toutes les données qu'il possède.

Apprentissage renforcé

Ce mode d'apprentissage va compléter les précédents en vous proposant d'évaluer, au fil de l'eau, les informations fournies par l'algorithme. L'algorithme tiendra compte de votre rétroaction pour ses futures décisions. Ce mode est là aussi très adapté à l'AIOps, car il s'insère facilement dans une GUI (Graphical User Interface) d'outils d'administration. Ici, l'algorithme vous remontera peut-être que les 10 Mbit/s en plus sont une anomalie, mais vous aurez la possibilité d'indiquer que cette information n'est pas pertinente. Le comportement sera automatiquement ajusté selon vos souhaits.

2.1.2 Au-delà de l'apprentissage…

En pratique, un travail conséquent sur la présentation des données et leur agrégation est à faire au préalable pour avoir des résultats probants : on ne peut décidément pas laisser la machine toute seule ! Dans l'AIOps, ce travail incombe le plus souvent à l'éditeur logiciel puisque peu d'équipes informatiques sont capables de mettre en place ce type de solutions par elles-mêmes. Comme nous le verrons plus tard, c'est la pertinence de la donnée utilisée pour l'apprentissage qui va rendre un algorithme efficace.

2.1.3 Absence de tout sens commun

Il est important de rappeler que l'algorithme est dénué de tout sens commun : ce qui vous semblera évident ne l'est pas forcément pour une machine.

Prenons la phrase suivante : « Je n'ai pas pu mettre la valise dans la voiture, car elle est trop grosse ». En tant qu'humain, vous savez que, dans ce contexte, c'est la valise qui est trop grosse. La machine, quant à elle, ne peut pas le deviner. On voit donc que le *Machine Learning* ne fera pas de miracles sans un minimum de gardes fous. Là aussi, il incombe à l'éditeur logiciel de compléter l'intelligence artificielle avec d'autres algorithmes plus traditionnels pour que le résultat ait un sens.

2.1.4 Corrélation n'implique pas causalité !

Si les algorithmes vont pouvoir déterminer les corrélations entre plusieurs variables (ou événements), il faudra se méfier de tirer des conclusions trop hâtives quant aux relations de cause à

effet. Deux variables peuvent très bien évoluer ensemble mais être causées par un troisième facteur. Prenons par exemple, un algorithme qui trouverait une corrélation entre une augmentation de CPU sur un routeur, et un accroissement simultané des pertes de paquets. Il serait tentant d'affirmer que c'est l'augmentation de CPU qui cause les pertes de paquets… Mais il est tout à fait probable que ces 2 éléments soient la conséquence d'une troisième cause : une augmentation de trafic qui causerait à la fois une élévation de la CPU et des pertes en raison de congestion sur une liaison au début, trop basse. Là aussi, il incombe à l'éditeur logiciel de compléter les résultats rendus par une intelligence artificielle avec les fonctions nécessaires pour pallier ces difficultés.

2.1.5 Domaines d'application du *Machine Learning*

Il y a des domaines dans lesquels le *Machine Learning* est parfaitement adapté : détection de déviation par rapport à des états standards, comparaisons multiples, corrélation de multiples facteurs pour mettre en évidence des problèmes qui n'ont pas de mécanismes bien connus, création de groupes à partir d'échantillons, détection de saisonnalité… Ici, la promesse est de pouvoir déterminer des modèles qui pourront ensuite être utilisés pour améliorer l'infrastructure système et réseau. Anticiper les évènements avant qu'ils ne soient vus, c'est une des grandes promesses du *Machine Learning.*

2.2 Machine Reasoning

Le *Machine Reasoning* consiste à automatiser des actions et une logique humaine préalablement définie. Ici, l'objectif n'est pas de déterminer un modèle mais de faire faire à la machine ce qu'on aurait fait avec notre logique humaine. On va nourrir notre automate avec ce que l'on appelle des ontologies. Les ontologies sont directement élaborées à partir d'expertise humaine. On n'a plus de notion d'apprentissage avec le M*achine Reasoning* : on connaît le modèle et on l'applique. Supposons, par exemple, que nous savons qu'une CPU supérieure à 80 % combinée à une mémoire de plus de 75 % qui engendre un risque de crash important, il est possible de définir une nouvelle ontologie avec ces paramètres. L'algorithme de *Machine Reasoning* va rapidement détecter les équipements qui remplissent cette condition et vous alerter. Évidemment, l'objectif est de pouvoir adresser des chaînes de vérifications largement plus complexes et qui sont pénibles à réaliser à la main. Pensez à toutes les fois où vous avez cumulé les « *show commands* » sur tout un ensemble d'équipements pour détecter l'origine d'un problème de performance : vous avez suivi une logique précise. C'est cette dernière qui peut être modélisée et vous fera gagner un temps incroyable. Dans le cas du *Machine Reasoning*, on sait exactement ce que l'on va chercher et les problèmes que l'on va mettre en évidence.

Bien que moins innovante de prime abord, cette approche est très pertinente dans un contexte AIOps pour lequel on a déjà des modèles bien précis, déterminés par des équipes de support compétentes. Il serait dommage de se priver du *Machine Reasoning* qui va de manière pragmatique déjà assurer la base et vous aider dans le champ des problématiques connues.

Le *Machine Learning* va devenir particulièrement intéressant voire indispensable :

– quand on n'est pas capable de déterminer des ontologies ;

– pour découvrir d'autres éléments qui nous auraient échappé avec les modèles connus.

En pratique, un logiciel intégrera certainement toutes ces approches *Machine Learning/Reasoning* et de nombreux algorithmes pour vous fournir des résultats pertinents. C'est le résultat qui compte avant tout.

2.3 Et le Deep Learning ?

Le *Deep Learning*, ou apprentissage profond, peut être vu comme une évolution du *Machine Learning*, car les principes restent les mêmes : l'algorithme va permettre d'apprendre et découvrir un modèle. Les algorithmes utilisés permettent d'exploiter davantage de données et de faire des analyses plus poussées. Alors que le *Machine Learning* est, à la base, guidé par des *data scientists* qui vont paramétrer des algorithmes, le *Deep Learning* est plus autonome et peut chercher des éléments que nul n'aurait imaginés. Une autre grande différence est que, si le *Machine Learning* utilise en source / destination des données structurées et principalement numériques (par exemple un tableau avec l'évolution de la température d'un équipement dans le temps), le *Deep Learning* va pouvoir exploiter des données non structurées (par exemple des logs, ou des exports bruts de statistiques). L'étape la plus difficile dans le *Machine Learning* est de faire en amont le tri des données à envoyer à l'algorithme : sélectionner les données et les agréger. La promesse du *Deep Learning* est de s'épargner cette étape pour travailler sur des données brutes. C'est, en ce sens, que le *Deep Learning* est utilisé pour l'analyse d'images brutes, la génération de texte instantané lors d'une conversation…

Le *Deep Learning* n'a pas vocation à remplacer le *Machine Learning*, notamment dans l'AIOps, pour lequel, on reste principalement sur l'analyse de données numériques avec des schémas statistiques bien établis. Le *Deep Learning* peut apporter un complément bienvenu pour trouver des éléments que nul pourrait prédire.

3 Déterminer la pertinence d'un algorithme

L'évaluation des algorithmes se fera en analysant leur « précision » et leur « rappel » [3].

3.1 Précision

Un algorithme va faire des prédictions dont certaines vont être vraies, et d'autres fausses (on parle aussi de faux positifs). La précision est le ratio entre le nombre de prédictions vraies et le nombre total de prédictions. Un algorithme qui aura une précision proche de 1 sera donc très fiable : tout ce qu'il dit (ou presque) est vrai. On peut donc lui faire confiance.

3.2 Rappel

Le rappel (*recall* en anglais) consiste à évaluer si l'algorithme a bien fait toutes les prédictions possibles dans le jeu de données fourni. C'est le ratio entre le nombre de prédictions faites et le nombre total de prédictions qui auraient pu être faites. Un rappel proche de 1 montre que l'algorithme a bien trouvé tout ce qu'il y avait à découvrir.

3.3 Que choisir… précision ou rappel ?

Le monde parfait dans lequel un algorithme aurait à la fois une précision et un rappel de 1 n'existe pas. Plus on va améliorer le rappel, moins on aura de précision et vice versa. Dans le cadre de l'AIOps, quand on va chercher à remonter absolument tous les incidents réseau, on risque certainement de remonter des évènements normaux. Et si l'on veut être certain de ne pas avoir de faux positifs, alors il faut accepter de ne pas tout détecter… Pour l'AIOps, compte tenu du fait que les équipes systèmes et réseau manquent déjà de temps pour se pencher sur les problèmes réels, il convient d'avoir avant tout une précision maximale, peu importe que certains éléments ne soient pas vus. La sécurité pourrait légèrement déroger à cette règle en favorisant davantage le rappel, mais on voit en pratique que même dans ce domaine les administrateurs croulent déjà trop souvent sous les alertes et recherchent avant tout la précision.

4 La data, la base de l'IA

Un élément très important à noter est que le bon fonctionnement d'une intelligence artificielle repose avant tout sur la présence de données. Il faut des données en quantité et en qualité, qui reflètent suffisamment de cas concrets.

Dans le cadre du *Machine Reasoning* par exemple, tout repose sur la capacité du constructeur à fournir les ontologies. Ces dernières ne peuvent être établies qu'avec un minimum de connaissance et d'expérience. Une équipe de support ne va pouvoir créer des ontologies que s'il a suffisamment d'informations quant à ce qu'il faut chercher. Pour cela, elle va s'appuyer sur tous les incidents remontés jusqu'à présent. Sans données, il est impossible de créer des ontologies suffisamment abouties.

Pour le *Machine Learning* (et par extension le *Deep Learning*), c'est d'autant plus évident. Plus il y a de données plus il est possible de faire des analyses pertinentes. Les algorithmes utilisés par les différents éditeurs logiciels sont globalement équivalents. La pertinence d'une solution est surtout liée à la quantité et à la qualité des informations utilisées pendant la phase d'apprentissage.

Les analyses croisées des données entre plusieurs organisations (entreprises, institutions publiques…) sont essentielles pour gagner en pertinence. Cela fait bénéficier à l'un ce qui a été découvert en analysant les données des autres. On parle aussi de *crowdsourcing* : on bénéficie de l'intelligence collective. Le challenge, ici, est d'anonymiser les données sans perdre en pertinence. Les algorithmes ne travaillent pas sur des données réelles (par exemple des températures) mais sur des données transformées. Le *crowdsourcing* implique des plateformes colossales de collecte de données dans le *cloud*. Elles doivent garantir la sécurité et l'intégrité des données collectées.

Si AIOps semble faire le jeu des *startups*, c'est en pratique loin d'être le cas :

– les investissements nécessaires pour débuter sont considérables (nombreux *data scientists*, ressources de calcul et de stockage colossaux…) ;

– il faut de la donnée pour valider les modèles. Une *startup* qui n'a pas de base de client pourra difficilement déterminer des modèles et les valider ;

– l'anonymisation et la sécurisation des données dans le *cloud* implique une crédibilité et une renommée plus difficilement atteignable par des nouveaux acteurs.

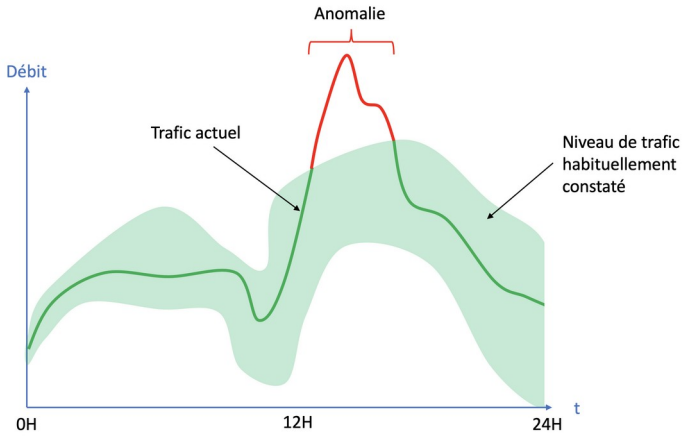
Seuls les acteurs disposant de suffisamment de données, provenant d'organisations suffisamment nombreuses variées, pourront bâtir des solutions efficaces. Aussi, une *startup* devra mettre en place des partenariats pour disposer de données nombreuses et variées.

5 Exemples d'applications pour l'AIOps

Cette section donne des exemples dans lesquels AIOps montre déjà des résultats intéressants. Ce n'est pas du tout exhaustif tant les possibilités sont immenses.

5.1 La sécurité

Le *Machine Learning* donne des résultats très pertinents pour la détection de menaces via l'analyse de flux inhabituels sur le réseau (volume, type…) Des augmentations soudaines de trafic d'un ou plusieurs utilisateurs peuvent être symptomatiques d'un vol de données ou de DDOS.

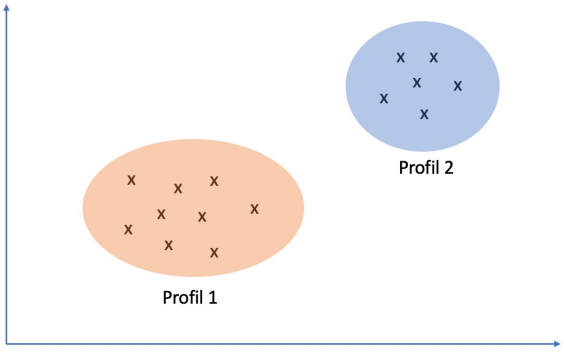


Détection de vol de données

De la même manière, le changement soudain de typologie de trafic (protocoles, destinations…) peut refléter une attaque ou une usurpation d'identité sur le réseau. Il sera également possible de cette manière de découvrir des clients « cachés » derrière un dispositif NAT.

5.2 *Profiling* de terminaux

Le *Machine Learning* peut être utilisé également pour la catégorisation des terminaux d'un parc, ceux-ci ayant eu tendance à se multiplier ses dernières années avec l'avènement de l'IoT. Ici, on utilisera la capacité du *Machine Learning* à catégoriser les clients en groupes selon certains critères de connexion (CDP, LLDP, MAC, DHCP…) mais également selon le trafic qu'ils génèrent. Une fois ce tri fait, il ne reste qu'à labelliser chacun d'entre eux et le tour est joué. Ici on pourra bénéficier du *crowdsourcing* pour bénéficier de la labellisation faite par une autre organisation. Il est fort probable que vous n'êtes pas le premier à utiliser un terminal, quand vous le déployez aussi il est quasiment certain que d'autres auront fait cette labellisation avant vous.



Machine Learning pour le profiling des équipements

On peut également utiliser ces mêmes principes pour détecter une déviation dans le résultat du *profiling* qui pourrait correspondre à une usurpation d'identité (*spoofing*).

5.3 Anticipation des problèmes de performance Wi-Fi

Un des challenges du Wi-Fi est d'arriver à évaluer quand le réseau n'est plus à même de fournir la performance attendue du fait par exemple d'une couverture insuffisante, d'un problème de perturbation radio (interférences…) Le *Machine Learning* là aussi, peut aider en détectant les

évolutions du nombre de clients connectés par point d'accès et en indiquant quand la tendance annonce que cela peut engendrer des risques sur la performance, nécessitant éventuellement de revoir le *design* de la zone concernée (ajout de points d'accès, ajout de radios…)

Dans ce cas de figure, on comprend l'intérêt d'une prédiction tant le changement d'un *design* radio peut prendre du temps. Être capable d'anticiper est vital, car il permet d'agir avant que les utilisateurs ne remarquent un problème. Le *Machine Learning* peut aussi grandement aider pour la détection des point d'accès « rogue », des problèmes sur l'affectation des canaux… Les bénéfices sont nombreux.

6 Vers un Internet prédictif ?

C'est tout l'objet de plusieurs articles [4] [5] [6] publiés par JP Vasseur, Fellow chez Cisco Systems, qui a mené des études de performance sur Internet avec de nombreux *data scientists* en utilisant le *Machine Learning*. Il s'est appuyé pour cela sur les performances remontées de nombreux tunnels Cisco SD-WAN, après avoir obtenu l'accord des clients concernés. Les objectifs sont nombreux :

– trouver des anomalies non détectables via des moyens ordinaires ;

– déterminer l'origine d'incidents. On comprend, ici, l'importance d'avoir une vue croisée entre plusieurs clients pour détecter des problèmes chez des opérateurs ;

– déterminer s'il est possible d'anticiper des problèmes sur Internet en découvrant une saisonnalité.

Les résultats montrent que s'il existe naturellement des pannes qui ne peuvent pas être anticipées (comme certaines coupures d'électricité ou coupures de lien…) une grande partie des problèmes peut l'être. Sur certains liens, il a été possible de prédire jusqu'à 90 % des moments, durant lesquels, les performances n'étaient pas au rendez-vous. L'étude a montré qu'un re-routage ad-hoc réalisé sur la base de ces données aurait permis une continuité de service pour les applications les plus critiques.

On comprend aisément que l'analyse de millions de chemins Internet requiert des moyens colossaux. Mais l'enjeu en vaut la chandelle tant la promesse de pouvoir maîtriser la qualité de service sur des liaisons Internet peut avoir des impacts gigantesques sur les architectures réseau des prochaines décennies. Cela illustre à quel point les enjeux de l'AIOps dépassent largement les opérations de base, mais peuvent transformer notre manière de concevoir les infrastructures IT.

7 Démarrer avec l'AIOps

Utiliser un produit sur étagère ou faire soi-même, telle est l'éternelle question à laquelle les équipes systèmes et réseaux sont confrontées. On ne compte pas les scripts de configuration, ou autres *weathermaps* maison qui permettent de répondre à un besoin dans un contexte précis.

L'AIOps va naturellement susciter les mêmes questionnements : faut-il investir dans des produits ou créer soi-même sa propre solution. Ici, il faut rappeler que l'AIOps reste globalement jeune et que les investissements nécessaires sont largement supérieurs à ceux requis pour de la supervision simple ou des projets d'automatisation. On rappellera à nouveau que seuls 15 % des projets liés à l'intelligence artificielle voient le jour en production après des cycles longs de développement et de validation. Si un investissement peut tout de même se justifier quand les retombées sont gigantesques (*trading*, optimisations de production…) il va être compliqué de tenter l'expérience dans des équipes disposant déjà de peu de moyens. La difficulté pour vous lancer, sera le manque de

data : vous n'aurez que vos propres données pour créer/valider vos modèles et cela se montrera certainement insuffisant avec des risques importants de faux positifs/négatifs.

Aussi, pendant encore quelques années, il est plus que probable que seules les équipes réseau et système très importantes (quelques fournisseurs de service et très grandes entreprises) auront la capacité de créer elles-mêmes leur propre solution. Mais, dans l'ensemble, ce sont bien des produits sur étagère, utilisant du *Machine Learning* qui seront déployés. Pour l'utilisateur final, il faudra surtout aller au-delà de la terminologie AIOps qui devrait être utilisée à tort et à travers pour se pencher réellement sur les bénéfices réels des solutions.

Bibliographie

[1] Rob van der Meulen, Thomas McCall, Gartner, Gartner Says Nearly Half of CIOs Are Planning to Deploy Artificial Intelligence. https://www.gartner.com/en/newsroom/press-releases/2018-02-13-gartner-says-nearly-half-of-cios-are-planning-to-deploy-artificial-intelligence. Mars 2018.

[2] Business & Décision. Intelligence Artificielle - Restez maître de votre futur. Mars 2021

[3] Précision et Rappel. Wikipedia. https://fr.wikipedia.org/wiki/Précision_et_rappel.

[4] Vinay Kolar, Ph.D., Principal Engineer ,JP Vasseur, Ph.D., Cisco Fellow, Mukund Raghuprasad. Large-scale Internet Path modelling and applications. Septembre 2020

[5] JP Vasseur, PhD, Cisco Fellow. From Dark to Grey Failures in the Internet. Juin 2021

[6] JP Vasseur, PhD, Cisco Fellow. Towards a Predictive Internet. Septembre 2021