opengear
A DIGI COMPANY

COMMENTAIRE DE RECHERCHE

Mesurer le coût réel des pannes de réseau

Le bon fonctionnement d'un reseau resilient est indispensable au succes d'une organisation aujourd'hui. En case d'indisponsibilite de ce dernier, la productivité diminue, l'entreprise est financièrement impactée et sa réputation en souffre. Or les tendances actuelles, telles que le travail à distance et la virtualisation, bien qu'elles contribuent à accroître la flexibilité et la productivité de l'entreprise, peuvent également rendre le réseau plus vulnérable aux pannes et aux attaques.

Face à une industrie informatique plus virtualisée, notamment avec la migration actuelle vers le cloud, la montée en puissance de la connectivité et l'émergence de l'Internet industriel des objets (IIoT), la gestion des réseaux devient de plus en plus compliquée et onéreuse. À mesure que le nombre de personnes qui télétravaillent ou se connectent à distance augmente (une tendance susceptible d'être accélérée par la crise sanitaire actuelle), elle se disperse davantage. Ensemble, ces développements font qu'il est encore plus important que le réseau reste opérationnel, mais aussi plus probable que des pannes se produisent.

LA CAUSE DES PANNES

Les organisations ne cessent de complexifier leurs réseaux, ce qui tend à les rendre plus vulnérables. Aujourd'hui, il existe une série de facteurs qui peuvent provoquer des pannes de réseau ou de système, des problèmes de transporteur FAI aux coupures de fibre en passant par la simple erreur humaine. À côté de cela, les périphériques réseau deviennent de plus en plus complexes, ce qui rend la réalisation d'une sécurité réseau robuste plus difficile.

Les piles de logiciels devant être mises à jour plus souvent, elles deviennent plus vulnérables aux bogues et aux cyberattaques. Il existe, d'une part, un risque d'attaques externes venant de cybercriminels désireux d'exploiter les faiblesses du réseau d'entreprise ou de bots externes constamment à la recherche de vulnérabilités leur permettant de pénétrer les réseaux d'entreprise et, d'autre part, une menace croissante émanant des employés de l'entreprise eux-mêmes. Les causes sont tout aussi diverses que les risques : employés mécontents qui ouvrent délibérément les portes aux cybercriminels ou utilisateurs de bonne foi qui sont victimes d'attaques de phishing.

Enfin, l'expansion constante des réseaux englobant l'informatique de périphérie a conduit à un transfert accru des calculs en périphérie (par ex. les services du dernier kilomètre comme Netflix) et à la mise en place d'équipements plus complexes dans des endroits éloignés, où il n'y a pas de personnel informatique et où la redondance n'est pas possible. En pareil cas, il ne suffit plus simplement de concevoir un centre de données robuste. Le réseau n'est pas plus solide que son point le plus faible. Le développement de l'informatique de périphérie nécessite donc de repenser complètement le réseau.

Tout cela contribue à augmenter l'intensité des pannes de réseau. Dans une récente étude indépendante de 500 responsables informatiques commandée par Opengear et réalisée par OnePoll, plus de la moitié (51 %) des personnes interrogées ont déclaré que leur organisation avait connu au moins quatre pannes d'une durée de plus de 30 minutes au cours de l'année écoulée. En effet, près d'une personne sur cinq (18 %) a déclaré avoir subi au moins sept pannes de ce type au cours des 12 mois précédents. De plus, près des deux tiers (65 %) des répondants ont déclaré que le nombre de pannes subies par leur organisation avait augmenté au cours des cinq dernières années.

La fréquence et la durée des pannes ont par ailleurs un impact financier important sur les entreprises. Près d'un responsable informatique sur trois (31 %) dans le monde a déclaré que les pannes de réseau avaient coûté à leur entreprise plus de 1,2 million de dollars au cours des 12 derniers mois et un sur six (17 %) a déclaré que cela leur avait coûté 6 millions de dollars ou plus. Par ailleurs, moins d'une personne sur dix (8 %) était en situation d'affirmer que ces pannes ne leur avaient rien coûté du tout pendant cette période.

BESOIN D'UNE RÉPONSE RAPIDE

En plus des difficultés auxquelles elles sont confrontées, il est souvent difficile de résoudre ces pannes rapidement. 38 % des personnes composant l'échantillon de recherche ont déclaré qu'il fallait en moyenne plus d'un jour ouvrable à leur organisation pour trouver et résoudre une panne de réseau une fois qu'elle avait été signalée.

L'absence de planification est un problème. Plus de la moitié (59 %) des organisations interrogées n'ont pas mis en œuvre de programme d'entretien préventif pour minimiser les temps de panne. Avec de nombreux réseaux dispersés, il n'est pas surprenant que pour 41 % des répondants à l'enquête le « temps de trajet pour faire intervenir des ingénieurs sur le site » figure parmi les deux défis principaux auxquels ils sont confrontés pour résoudre rapidement un problème de réseau. Compte tenu du temps nécessaire pour résoudre les pannes de réseau et des coûts encourus, trouver une solution est devenu une priorité absolue.

POURQUOI LA RÉSILIENCE EST LA SOLUTION

Face à tous les défis énumérés ci-dessus, se développe aujourd'hui un concept connu sous le nom de résilience des réseaux. Mais qu'entend-on exactement par là ? Pourquoi est-ce important et comment y parvenir au mieux ? Il existe un nombre incalculable de définitions.

Pour Joshua Sanders, de Lending Tree : « La résilience du réseau est un moyen de minimiser les interruptions. » Et si le réseau tombe en panne, avoir un moyen d'y accéder et ne pas avoir à se rendre sur place pour réparer le réseau. »

Chris Weindel, d'Eldorado Resorts, a ajouté : « La résilience du réseau désigne la rapidité avec laquelle vous pouvez vous remettre après une panne. N'est-ce pas ? Le réseau hors bande est notre dernière ligne de défense. Nous espérons ne jamais devoir l'utiliser, mais nous sommes heureux de l'avoir en cas de besoin. »

Pour nous, chez Opengear, la résilience des réseaux consiste en la « capacité de fournir et de maintenir un niveau de service acceptable face aux défauts et aux défis du fonctionnement normal ». Il s'agit de notre définition officielle, que l'on peut résumer ainsi : la « capacité de résister et de se remettre d'une interruption de service ». Une manière de la mesurer est la rapidité avec laquelle l'entreprise peut reprendre un fonctionnement à capacité normale après une panne.

Quelle que soit la définition exacte, la plupart des gens savent que la véritable résilience réseau ne peut être obtenue en assurant la résilience d'un seul équipement, qu'il s'agisse d'un commutateur central ou d'un routeur. Il faut, au contraire, que toute solution de résilience puisse se connecter à tous les équipements d'un site périphérique ou d'un centre de données, cartographier ce qui existe et déterminer ce qui est hors ligne et en ligne à tout moment.

Une des priorités doit être de s'assurer qu'une entreprise ait la visibilité et l'agilité nécessaires pour faire face aux problèmes à mesure qu'ils surviennent. Prenons l'exemple d'une grande entreprise de finance ou de santé dotée d'un centre d'opérations réseau (NOC) dont les applications et le service client doivent être constamment disponibles. Il se peut très bien qu'elle ait plusieurs succursales à travers le monde et connaisse des problèmes de fuseau horaire. Elle peut donc rencontrer des difficultés ne serait-ce que pour détecter une panne lorsqu'elle se produit, puisqu'elle ne reçoit pas d'alerte quand le réseau est interrompu. Même si elle parvenait à déceler la panne, il lui serait difficile de savoir quelle partie de l'équipement pose problème et à quel endroit, sans envoyer quelqu'un sur place pour une inspection.

ÉTENDRE LE RÔLE DU HORS BANDE ET DE NETOPS

Pour résoudre les erreurs, une organisation peut avoir besoin d'effectuer un redémarrage rapide du système à distance. Si cela ne fonctionne pas, il peut s'agir d'un problème avec une mise à jour logicielle. C'est là que le concept de hors bande entre en jeu. Le réseau intrabande traditionnel suppose que la gestion des périphériques s'effectue via les protocoles courants tels que telnet ou SSH, en utilisant le réseau lui-même comme support. La gestion hors bande (OOB) offre une niveau de protection supplémentaire entièrement séparé du réseau, c'est pourquoi elle peut accéder et réparer rapidement tout équipement affecté si le système est verrouillé (ce qui est particulièrement important, par exemple, lors d'une cyber-attaque).

Les problèmes de réseau, ainsi que les difficultés de mise à jour logicielle évoquées ci-dessus, peuvent donc être résolus en utilisant la dernière fonction *Smart* OOB puisqu'il est possible de conserver une image de l'équipement principal et de sa configuration, et de reconfigurer rapidement l'appareil à distance sans avoir besoin de déployer du personnel sur le site (un facteur particulièrement important aujourd'hui compte tenu des restrictions de voyage dues à la pandémie de coronavirus.

En cas de panne, il est également possible d'offrir la résilience en basculant vers Cellular ™. Cela permet aux services essentiels de l'entreprise de rester opérationnels pendant que le problème d'origine est résolu à distance, même lorsque le réseau principal est en panne.

Même si l'intégration d'une résilience supplémentaire via OOB coûte de l'argent, le retour sur investissement peut considérablement dépasser les dépenses. Ce chemin d'accès alternatif ne peut être utilisé par une organisation que de manière occasionnelle, mais il constitue un facteur de succès incontournable lorsque cela est nécessaire. Il faut également noter que la résilience engage généralement beaucoup moins de dépenses que l'installation de nombreux équipements redondants. Ceci devient de plus en plus vrai à mesure que le déploiement des emplacements périphériques se développe. Bien qu'il soit possible pour une entreprise d'acheter de la redondance dans un centre de données, cette même redondance ne peut pas être intégrée au stockage des données dans un petit emplacement éloigné.

L'étude indique que le gain de temps (selon 45 % des répondants) et les économies de coûts (selon 41 % d'entre eux) constituent les deux principaux avantages dont bénéficient les organisations qui possèdent une solution capable de fonctionner indépendamment du réseau principal intrabande, ils permettent également de détecter et résoudre automatiquement les problèmes de réseau.

Pour résoudre les erreurs, une organisation peut avoir besoin d'effectuer un redémarrage rapide du système à distance. Si cela ne fonctionne pas, il peut s'agir d'un problème avec une mise à jour logicielle. Heureusement, cela peut également être résolu en utilisant la dernière fonction *Smart* OOB™ puisqu'il est possible de conserver une image de l'équipement principal et de sa configuration, et de reconfigurer rapidement l'appareil à distance sans avoir besoin de déployer du personnel sur place.

Au-delà d'offrir une solution de sauvegarde à toute épreuve grâce aux fonctions de gestion *Smart* OOB et Basculement vers Cellular, les organisations peuvent assurer une protection supplémentaire et réaliser des économies en ajoutant des outils tels que l'automatisation NetOps pour un provisionnement hors site sécurisé. Cela permet d'éliminer bon nombre de tâches répétitives, de minimiser le risque d'erreur humaine et de libérer du temps. Ainsi, 43 % des personnes interrogées dans le cadre de l'étude ont déclaré qu'elles « augmentaient le niveau d'automatisation du réseau » pour accroître la résilience du réseau au sein de leur organisation. Notons également que 89 % des répondants ayant adopté une automatisation NetOps ont déclaré que cela avait rendu le réseau de leur organisation plus fiable.

ALLER AU-DELÀ DE L'INTRABANDE POUR RÉSOUDRE LES COUPURES DE RÉSEAU

Les coupures de réseau constitue un problème majeur pour les plupart des grandes entreprises. Les pannes sont fréquentes et onéreuses en termes de temps et d'argent pour les entreprises, sans oublier qu'elles peuvent leur coûter leur réputation. Or la planification préventive fait défaut, et les entreprises dépensent souvent des sommes considérables pour remettre l'organisation sur pied, et notamment pour envoyer des ingénieurs sur des sites éloignés.

Dans ce contexte, une solution capable de fonctionner indépendamment des réseaux de production, de détecter et de résoudre les problèmes de réseau de manière automatique se révèle un atout précieux. La voie à suivre ? Une stratégie basée sur la résilience du réseau, soutenue par une gestion *Smart* OOB dans le cadre d'une automatisation NetOps.

MÉTHODOLOGIE DE SONDAGE

Les données sont basées sur une enquête auprès de 500 décideurs informatiques seniors situés en Amérique du Nord et en Europe. L'étude a été commandée par Opengear et menée par OnePoll, membre de l'AAPOR, en janvier 2020.

opengear
A DIGI COMPANY

MESURER LE **VRAI COÛT** DES

PANNE DE RÉSEAU

Un réseau résilient est essentiel au succès d'une organisation. Chaque fois qu'il n'est pas disponible, la productivité diminue, l'entreprise est financièrement impactée et sa réputation en souffre. Les organisations ne cessent de complexifier leurs réseaux, ce qui tend à les rendre plus vulnérables.

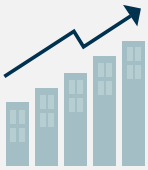
Une récente étude mondiale* sur les décideurs informatiques seniors, commandée par Opengear, a découvert :

31%

ont **perdu plus de 1 million de dollars** au cours des 12 derniers mois en raison de pannes de réseau

83% ont déclaré que la résilience du réseau était leur priorité absolue **#1**

23 % ont signalé une **augmentation de 25 % ou plus** du nombre de pannes de réseau au cours des 5 dernières années



39 % des pannes de réseau ont été résolues en plus d'un jour

42% ont déclaré que le **déplacement des ingénieurs** constituait l'élément le plus difficile à résoudre

Les entreprises du monde entier reconnaissent que la capacité à fonctionner indépendamment du réseau de production, **détecter et résoudre automatiquement les problèmes de réseau peut considérablement :**

améliorer la sécurité en **48%**

gagner du temps en **45%**

réduire les coûts en **41%**

Le déploiement d'une solution de résilience de réseau qui répond à ces problèmes est une priorité absolue

Faites le choix de la résilience : choisissez *Smart* Out-of-Band d'Opengear

opengear **ÉTATS-UNIS :** +1 888 346 6853 | **APAC :** +61 7 3871 1800 | **ROYAUME-UNI :** +44 20 4539 0280 | sales@opengear.com | www.opengear.com