Engineering Simplicity

eGuide

# Dépannage WAN : eGuide pour une résolution accélérée

Entrer

# Introduction

**Les WAN (réseaux étendus) sont des clouds complexes qui acheminent toute sorte de trafics, essentiels ou non, pour les activités.**

La plupart des WAN dépendent de fournisseurs de services et exploitent différents types de transport sous-jacent. Ces dernières années, les circuits d'accès Internet dédiés (DIA) sont de plus en plus utilisés pour construire et compléter les WAN à moindre coût.

Dans certains cas, les WAN sont même entièrement construits en tant qu'overlays ou VPN sur ces circuits Internet. Le trafic partage alors un accès avec le breakout Internet local plutôt que d'utiliser des connexions privées.

Il est essentiel d'observer et de surveiller le WAN (composants inclus) pour garantir la confidentialité, l'intégrité et la disponibilité du trafic professionnel.

La plupart des WAN reposent, directement ou indirectement, sur des protocoles de routage dynamique. Ces protocoles tiennent compte des défaillances éventuelles liées aux éléments sous-jacents et, le cas échéant, de la disponibilité à travers les différentes routes.

Même si les défaillances ne sont pas systématiques, elles sont favorisées par toutes les sources d'erreur potentielles : équipements, encombrements, défauts de câbles ou encore erreurs humaines.

Avec la démocratisation de l'automatisation et des niveaux d'abstraction constamment élevés, des problèmes logiques ou de routage font parfois obstacle à la continuité des services.

**Cet eGuide présente plusieurs mesures et approches concrètes pour faire face aux situations imprévues.**

**En cas de problème, plusieurs approches peuvent vous aider à rétablir le service.**

**L'objectif est toujours le même : réduire le MTTR tout en optimisant le MTBF.**

**Comment les risques sont-ils répartis sur votre WAN ?**

**Comment les classer ?**

**Que faire pour gérer les répercussions de ces inévitables défaillances ou encombrements ?**

# Approches de dépannage

**On décrit souvent Internet (ou les réseaux IP) comme une « série de tubes ». Mieux vaut peut-être l'imaginer comme une série de sessions et de messages échangés entre des groupes d'appareils gérés et non gérés.**

**Un concept d'« état » peut s'appliquer aux sessions, même si ce n'est pas le cas des messages. Ces deux types de trafic créent et utilisent de nombreuses dépendances, qui elles-mêmes entraînent des risques.**

Pour dépanner, il faut effectuer des vérifications et des recherches. L'une des méthodes de dépannage les plus efficaces consiste à constamment diviser l'espace du problème par deux, de la même façon que la recherche dichotomique. Bien sûr, vous pouvez valider au fur et à mesure de votre dépannage, mais les symptômes, les rapports de problème et le suivi ne reflètent pas nécessairement l'état du problème de base.

Les ingénieurs doivent souvent utiliser une méthode de corrélation pour orienter leurs efforts et rechercher la cause précise. Le but étant de découvrir la cause première aussi rapidement que possible, de la classer ou de la confiner, puis de mettre en place des mesures correctives pour éviter qu'elle ne se reproduise.

Le dépannage peut s'effectuer selon une approche « descendante » ou « ascendante », mais les deux méthodes, loin d'être parfaitement efficaces, sont parfois infructueuses ou trop longues. Une approche « intermédiaire », permet d'obtenir des résultats plus rapides, même si les conditions de départ sont floues.

Lorsque les ingénieurs (ou le système) reçoivent une alerte indiquant qu'il y a un problème, une vérification impartiale ou secondaire est généralement requise. C'est la mise en pratique du principe « faire confiance, mais vérifier ». Même si l'alerte d'erreur est légitime, il y a toujours des doutes à lever avant de se lancer dans un dépannage coûteux.

**Dans la plupart des phases de validation et de vérification, l'automatisation présente des avantages : un effort de travail réduit, des résultats plus rapides et plus de temps à consacrer aux interactions complexes de niveau supérieur pour les opérateurs humains.**

# Surveillance utilisateur

**La formule « On ne peut gérer ce qu'on ne peut mesurer » est avérée pour les réseaux. Aussi, une bonne visibilité sur vos actifs et vos services est essentielle, tout comme le filtrage des données pour éliminer les informations inutiles.**

**Il est donc important de trouver un juste équilibre entre le besoin de mesurer tous les éléments qui permettent d'identifier l'état, et la capacité de hiérarchiser les alertes rapidement exploitables.**

**Exploiter les sessions utilisateur**

Les utilisateurs se soucient de leurs données et sessions personnelles. Ils utilisent des appareils complexes sur lesquels ils exécutent tout un éventail d'applications qui peuvent être difficiles à dépanner. Lorsqu'ils rencontrent des problèmes, ils peuvent croire que le réseau ne fonctionne pas, sans qu'il ne soit de leur ressort, ni même de leur responsabilité, d'identifier la provenance de la défaillance technique.

Et même si les utilisateurs signalent parfois les problèmes de manière inexacte, ils n'en restent pas moins, grâce à leurs appareils, des indicateurs extrêmement précieux pour identifier les défaillances. Leurs sessions, qui révèlent le véritable état du WAN, peuvent vous aider à déterminer rapidement l'origine du problème.

Des groupes de contrôle peuvent être créés à partir des sessions des utilisateurs pour identifier les problèmes du réseau, qu'ils soient individuels ou globaux. Il y a encore peu, il était coûteux de suivre et de mesurer ces derniers.

Bien sûr, le dépannage manuel traditionnel est encore d'actualité, mais notre boîte à outils permet désormais de mieux diagnostiquer les situations qui représentaient auparavant un gouffre de temps et un enchevêtrement de responsabilités.

**Il est désormais possible de mettre en œuvre le Real User Monitoring sur le WAN et d'automatiser le dépannage « ascendant ». La vitesse de diagnostic s'en voit accélérée, et les défaillances WAN sont classées, pour une résolution des problèmes et un rétablissement des services plus rapides**.

# Surveillance et observabilité du réseau

**Un problème dont la source est connue n'a pas besoin de dépannage. Dans ce cas, il faut plutôt rechercher l'état indésirable dans les composants ou les éléments affectés.**

Avec une meilleure observabilité sur l'ensemble du réseau, il est plus facile de déterminer l'état du système à partir des données fournies, et de segmenter rapidement et précisément l'espace du problème pour trouver des solutions.

Les protocoles, les alertes, les datagrammes et les paquets sont tous clairement définis et doivent suivre des règles. Mais le réseau est pour sa part un système distribué complexe : la configuration d'un équipement influe sur l'état d'un autre équipement.

Traditionnellement, la surveillance réseau servait à contrôler l'état de santé des éléments réseau. Même si cette opération reste essentielle, il faut pouvoir prouver que les données de session d'un utilisateur donné peuvent être acheminées de manière fiable d'un point A à un point B.

En d'autres termes, il faut des données avec une meilleure cardinalité. Il incombe aux équipes opérationnelles de confirmer non seulement la disponibilité, mais aussi l'accessibilité des données du point de vue de l'utilisateur lors de l'acheminement.

Lorsqu'un système atteint un niveau de complexité tel que les dépendances et les états partagés empêchent d'identifier facilement la cause première, le fait est qu'il faut malgré tout dépanner.

- Les données fournies par les systèmes et les humains peuvent être correctes, mais elles risquent aussi d'introduire des bogues et des erreurs.
- Si un trop grand nombre de données sont recueillies, il y a un effet de surcharge. Et savoir où chercher à l'avance ne dispense pas pour autant d'une vérification.
- Si la surveillance permet de mesurer les états ou les limites problématiques connus, il faut souvent creuser plus loin pour déterminer la source du problème.

**Par définition, une défaillance encore non identifiée n'a pas été mesurée ou détectée. Cette démarche d'interrogation et de recherche est l'essence même du dépannage.**

**Plus un réseau est complexe, plus les facteurs susceptibles d'avoir un impact sur le trafic sont nombreux.**

**Et démontrer que le réseau fonctionne correctement devient une tâche délicate.**

# Dépannage WAN :

**Un WAN peut être composé de nombreux types de topologies, de protocoles, de fournisseurs et d'éléments.**

Voici quelques conseils et astuces essentiels pour faciliter votre tâche. Votre objectif doit être de rendre opérationnel votre propre processus de dépannage, en le structurant et en le documentant pour permettre un meilleur partage des connaissances et accélérer l'automatisation.

## Recommandations générales

Formulez toujours l'**énoncé du problème**, puis continuez de le préciser par la suite.

**Classez la portée et l'impact** en fonction des besoins de votre organisation et du degré de sévérité.

**Diagnostiquez et rétablissez la fonctionnalité aussi rapidement que possible.** Faites un bilan constructif si la cause d'origine reste indéterminée.

Demandez toujours à voir **des données récentes et des preuves empiriques**.

**Documentez au fur et à mesure.** Capturez et partagez (lorsque cela est permis) toutes les données, les extraits, les horodatages et les rapports.

**Revenez en permanence sur vos premières théories** quand vous cherchez à comprendre un problème.

Le principe de simplicité (ou rasoir d'Ockham) est vrai la plupart du temps. L'historique a aussi toute son importance : **qu'est-ce qui a changé ?**

Lorsque vous segmentez l'espace du problème, **concentrez-vous sur les différences** et les points communs.

Ce n'est pas parce que vous ne voyez pas quelque chose que cette chose n'existe pas.

Plus votre environnement est simple, plus il est facile à dépanner.

# Prérequis

**Les éléments réseau effectuent des contrôles de santé au niveau de l'équipement (y compris les équipements virtuels réunis).**

**Les interfaces sont surveillées et suivies, et les vitesses, seuils et statistiques des tampons ou de mise en file d'attente sont corrects**

**Il est possible d'utiliser traceroute à partir de l'emplacement de l'utilisateur.**

**L'accès aux tables de routage (RIB) et de transfert (FIB) est disponible pour tous les éléments réseau gérés concernés, y compris l'équipement de l'utilisateur si disponible.**

**La journalisation et les requêtes sont centralisées, de préférence avec un horodatage UTC indiquant les millisecondes.**

# Hypothèses

1. Le point de terminaison de l'utilisateur fait partie d'un groupe d'équipements présentant le même problème (plutôt qu'un problème lié à un seul hôte).
2. Les points de terminaison des utilisateurs transmettent bien le trafic vers d'autres destinations (sans traverser le WAN).
3. Toutes les données recueillies (isolées ou non) sont utiles mais potentiellement incorrectes jusqu'à ce qu'elles soient vérifiées ou contrôlées de manière impartiale dans un système de suivi.
4. Un problème WAN peut être continu ou intermittent.
5. Le problème provient du WAN, comme indiqué dans les points (1) et (2). Ce n'est pas un problème de routage, d'authentification ou de VPN côté client, etc.
6. La pile IPv4 est complète (par opposition à une pile double ou IPv6 uniquement).
7. La requête d'écho ICMP (type 8), la réponse d'écho (type 0) et le dépassement de délai (type 11) sont activés de bout en bout sur les éléments réseau du chemin source - destination.
8. Les équipes opérationnelles connaissent la configuration de leur topologie gérée. La documentation ou le mappage dynamique est à jour pour tous les nœuds d'infrastructure gérés.
9. La surveillance du réseau ne détecte aucun problème connu ou pertinent pouvant avoir un impact sur la période indiquée.

# Résolution et accessibilité

1. **Assurez-vous que les véritables adresses IP de l'interface source du client et du service à distance ou de la destination sont utilisées.** Il s'agit de s'assurer qu'une ressource désignée est bien utilisée pour comprendre comment elle se résout du point de vue du client.

2. **Envoyez un écho ICMP (ping) depuis l'adresse IP source de la passerelle par défaut du client vers l'adresse de destination** (avec le bit DF et une taille de paquet pouvant transiter de bout en bout). En cas d'échec...

3. **Tracez la route depuis l'IP source de la passerelle par défaut du client vers l'IP de destination** (utilisez UDP ou TCP si possible, autrement utilisez ICMP). En cas d'échec ou de nœuds imprévus...

4. **Assurez-vous que l'accessibilité IP suit le chemin escompté** et vérifiez le RIB du dernier « bon » saut connu.

5. **Vérifiez les listes de contrôle d'accès (ACL), les stratégies de pare-feu et les MTU de l'interface** sur le dernier « bon » saut connu, mais aussi pour les paquets en cours d'acheminement lorsqu'ils sont à un saut de distance.

6. **Si l'accessibilité de l'IP est démontrée, commencez par le sous-réseau source et testez les ports TCP ou UDP concernés pour le service en question.** S'ils ne sont pas disponibles sur l'équipement réseau, certains outils (telnet, tcptraceroute, tcping, curl, hping3, nmap ou nc) peuvent avoir besoin d'un accès à un équipement informatique polyvalent.

7. **Presque tous les services TCP répondront à un SYN**, mais de nombreux services UDP peuvent ne pas répondre si le message n'est pas correctement structuré pour le service en question.

8. **Vérifiez séparément que le service à distance écoute sur le bon port** (si possible) et répétez les étapes (1) à partir du sous-réseau à distance.

**Si vous ne contrôlez pas le point de terminaison source pour effectuer des tests en émulant complètement l'utilisateur, utilisez l'interface de couche réseau L3 initiale la plus proche (en général, la passerelle client par défaut).**

**Les éléments réseau comprennent généralement un sous-ensemble d'outils de dépannage en ligne de commande, mais ils ne sont pas toujours aussi flexibles que ceux des points de terminaison de calcul complets, où des packages et outils peuvent être installés.**

**Envisagez d'utiliser le Real User Monitoring (RUM) en plus de vos services courants pour avoir une visibilité sur les sessions en temps réel.**

# Prenez conscience des sessions et des applications

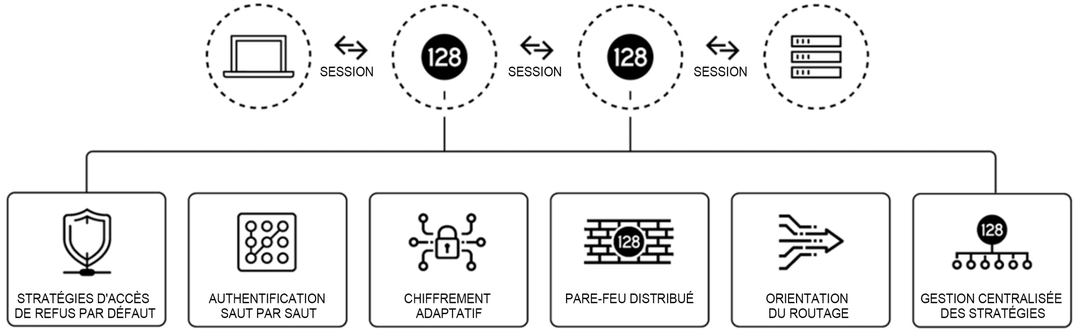
**Un bon dépannage se fonde sur une bonne connaissance de la situation. Traditionnellement, les routeurs accomplissent leurs tâches de transmission sans véritable concept d'état de session ou d'application. Les pare-feu et les équilibreurs de charge surveillent et exploitent certains aspects de l'état, mais les sessions ne sont pas reconnues sur l'ensemble du réseau. Imaginez si une nouvelle génération de routeurs pouvait reconnaître les sessions et des applications, et rendait ainsi le routage et l'application des stratégies plus intelligents ?**

Les routeurs Session Smart™ (SSR) de Juniper ont été conçus pour reconnaître les applications et les sessions.

L'expérience utilisateur est continuellement optimisée, ce qui permet de réduire les coûts d'assistance et le MTTR de 30 à 40 %. Avec ce modèle de mise en réseau basé sur les sessions, vous gagnez en performances sans devoir recourir aux tunnels et pouvez dimensionner le réseau simplement.

Un principe de sécurité « Zero Trust » est intégré à la structure, pour réduire considérablement les risques et assurer la fiabilité des services.

Grâce aux contrôles d'accès simplifiés et à l'hyper-segmentation, SASE (Secure Access Service Edge) est directement intégré.




**Quand l'intelligence fait partie intégrante de la structure du réseau, de nombreux avantages en découlent : réduction des coûts de support, meilleure visibilité, dépannage simplifié, etc.**

# Juniper Session Smart™

**La solution logicielle Session Smart™ de Juniper peut être déployée rapidement et facilement sur site (via une whitebox ou un hyperviseur) ou sur un cloud public.**

Ce modèle axé sur les sessions permet de mettre en place une structure sans limites qui réduit la latence jusqu'à 60 % et les coûts de bande passante de 30 à 50 %. Grâce à des options de déploiement flexibles, vous pouvez exploiter tous vos acquis et tirer avantage d'un WAN plus intelligent et plus simple : des utilisateurs plus satisfaits, de meilleures performances, moins de dépannage et une sécurité accrue.

### Simplicité

Pas de tunnel, pas de superposition, finis les réseaux reposant sur le matériel.

### Agilité

Déploiements plus rapides, meilleure réactivité, optimisation dynamique.

### Securité

Principe Zero Trust : authentification + chiffrement + segmentation.

### Performances

Moins de coûts, plus d'évolutivité, une optimisation dynamique.

### Économies

Réduction des coûts de bande passante et de connectivité.

# Découvrez le SD-WAN avec Session Smart™.

**Visionnez le webinaire**

**Participez à l'une de nos démos Transformation Thursday pour voir le SD-WAN augmenté par l'IA en pleine action.**

**Des questions ?**
**Pour une aide approfondie et des guides de dépannage détaillés, consultez notre base de connaissances.**

PN : 7400132-001-FR

**Siège social et commercial**
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089, États-Unis
Téléphone : 888.JUNIPER
(888.586.4737)
ou +1.408.7452000
Fax : +1.408.745.2100
www.juniper.net/fr/fr/

**Siège EMEA et APAC**
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, Pays-Bas
Téléphone : +31 0 207 125 700
Fax : +31.0.207.125.701

Copyright 2021 Juniper Networks, Inc. Tous droits réservés. Juniper Networks, le logo Juniper Networks, Juniper, Junos et les autres marques commerciales indiquées ici sont des marques déposées de Juniper Networks, Inc. et/ou de ses filiales aux États-Unis et dans d'autres pays. Les autres noms peuvent être des marques commerciales de leurs détenteurs respectifs. Juniper Networks décline toute responsabilité en cas d'inexactitudes dans le présent document. Juniper Networks se réserve le droit de changer, modifier, transférer ou tout autrement réviser la présente publication sans préavis.