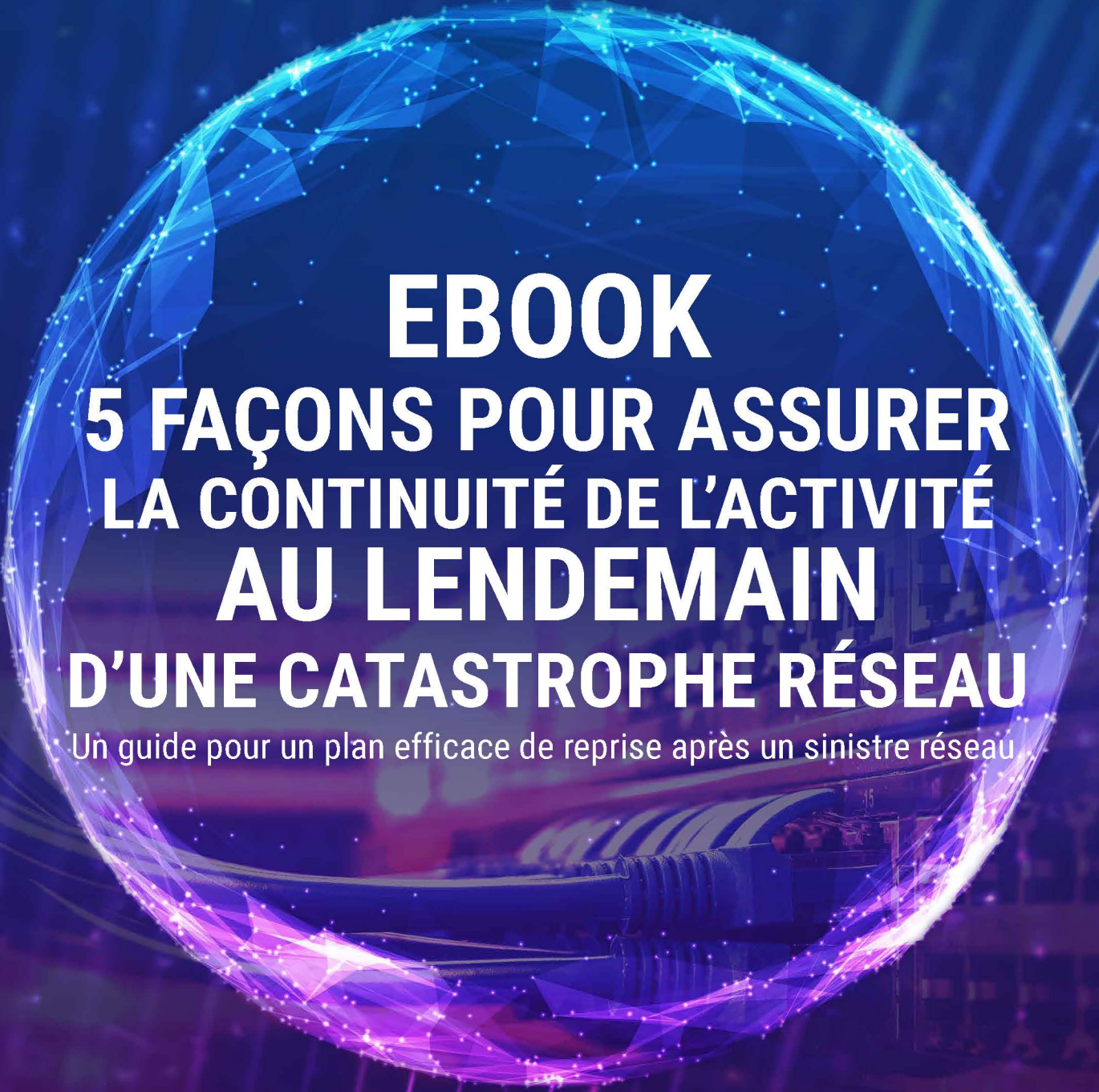




EBOOK **5 FAÇONS POUR ASSURER** **LA CONTINUITÉ DE L'ACTIVITÉ** **AU LENDEMAIN** **D'UNE CATASTROPHE RÉSEAU**

Un guide pour un plan efficace de reprise après un sinistre réseau

Introduction

Il est de notoriété publique que la gestion des réseaux n'est pas facile. Cependant, certaines personnes ne savent peut-être pas que de nombreux inconvénients mineurs rencontrés en environnement de travail peuvent être imputés à un problème de réseau. A première vue, la plupart des problèmes informatiques quotidiens peuvent ressembler à une série d'événements aléatoires et malheureux qui peuvent survenir n'importe quel jour au travail. Mais il est possible que tous ces problèmes aléatoires soient liés.

En tant qu'administrateur réseau, vous devez comprendre que de nombreux problèmes informatiques peuvent être réduits à quelque chose comme une simple erreur de modification sur un périphérique ou une vulnérabilité laissée sur un périphérique non vérifié. Ce n'est qu'après une analyse complète de votre réseau et l'identification de toute faille existante que vous pouvez résoudre un problème et restaurer votre réseau à son état opérationnel complet.

La gestion d'un réseau sans sinistre nécessite la maintenance et l'examen minutieux de divers segments de votre infrastructure réseau. Cependant, l'approche manuelle de ce travail est le meilleur moyen de faire face à une panne de réseau. Cet 'ebook' décrira quelques façons dont une panne ou une perturbation du réseau peut se produire et comment Network Configuration Manager, un outil de gestion de configuration, peut vous aider.

Une perte de bande passante dans le réseau

Les entreprises investissent souvent beaucoup d'argent dans l'acquisition de grandes quantités de bande passante pour leurs applications critiques. Cette bande passante est généralement partagée entre tous les utilisateurs du réseau de l'entreprise. Lorsqu'un membre du réseau utilise une application qui consomme une grande quantité de bande passante, il peut rendre le réseau indisponible pour les autres utilisateurs du réseau. Si l'application en question est utilisée pour des activités non commerciales, elle réduit le ROI du budget de bande passante alloué à l'entreprise.

Pour résoudre ce problème, il n'est pas recommandé de vérifier manuellement la consommation de bande passante de chaque utilisateur lorsque vous êtes déjà pressé par le temps pour résoudre un problème de réseau. Au lieu de cela, vous devriez mettre un plafond sur la quantité de bande passante que chaque utilisateur peut utiliser. Ainsi, la bande passante de votre entreprise sera répartie uniformément entre tous les utilisateurs et la productivité globale de votre entreprise n'en souffrira pas lorsqu'un seul utilisateur consomme une quantité démesurée de bande passante.



Selon l'enquête mondiale de la société britannique de sécurité informatique Sophos intitulée The Dirty Secrets of Network Firewalls, "En moyenne, 45% du réseau traffic est non identifié. Par conséquent, il ne peut pas être contrôlé."

La limitation de la bande passante pour chaque utilisateur peut être réalisée avec des listes de contrôle d'accès (ACL). Les ACL peuvent être utilisées pour contrôler la bande passante que chaque adresse IP peut consommer. Vous pouvez limiter la consommation de bande passante de plusieurs périphériques dans votre site en créant et en exécutant un configlet ACL avec Network Configuration Manager. Ce configlet devrait spécifier la limite de bande passante pour chaque adresse IP. Si nécessaire, vous pouvez également bloquer l'accès de certaines adresses IP à votre réseau, ce qui permet aux utilisateurs de bénéficier d'une connexion sans problème.

Une violation des normes de l'industrie

Dans l'industrie des réseaux, certaines normes ont été établies pour éviter que les périphériques réseau ne deviennent vulnérables. Toute violation de ces normes pourrait entraîner des problèmes tels que des atteintes à la protection des données, des pannes et une perte de réputation pour l'entreprise. C'est pourquoi lorsque les administrateurs réseau apportent des modifications à leur réseau, ils doivent garder à l'esprit que les périphériques de leur entreprise doivent être conformes à toutes ces normes. PCI DSS, HIPAA, SOX et Cisco IOS font partie des normes les plus importantes qui doivent être respectées. Si vous souhaitez que vos périphériques réseau adhèrent à des règles supplémentaires qui ne sont pas présentes dans les politiques mentionnées ci-dessus, vous pouvez créer une politique de conformité personnalisée avec Network Configuration Manager.

Par exemple, une recommandation générale dans le monde des réseaux est d'éviter d'utiliser TELNET. En effet, contrairement aux autres protocoles de communication, TELNET n'est pas chiffré, ce qui le rend très peu sûr. Ce manque de sécurité dans le protocole rend les équipements qui l'utilisent vulnérables aux piratages, ce qui entraînera éventuellement une panne de réseau. Vous devriez être instantanément notifié si quelqu'un active TELNET dans le réseau de votre entreprise, qui est l'endroit où les contrôles de conformité deviennent une assurance vie.



Selon un sondage de Newscycle Solutions, "Une étude approfondie de conformité PCI réalisée en mars 2015 par Verizon a révélé que 80% des entreprises échouent à leur première évaluation de conformité PCI".

Effectuer régulièrement des contrôles de conformité vous aidera à obtenir une meilleure visibilité sur les périphériques de votre réseau et à identifier ceux qui violent les politiques établies. Avec Network Configuration Manager, vous pouvez effectuer des contrôles de conformité sur les périphériques associés à chaque stratégie. Vous pouvez également choisir d'effectuer des tests ad hoc sur des périphériques suspectés d'être vulnérables.

Vous pouvez également créer des politiques de conformité personnalisées à titre de mesure préventive contre les indisponibilités du réseau qui surviennent parce que le protocole TELNET est activé. Cette politique personnalisée doit inclure une règle qui vérifie les périphériques dont TELNET est désactivé. Lorsque des vérifications de conformité sont effectuées pour cette politique, tous les périphériques qui utilisent TELNET seront identifiés, ce qui vous permettra de remédier rapidement à la situation. Réparer une violation comme celle-ci signifie normalement que vous devriez faire une recherche dans une énorme liste de scripts et ensuite exécuter le bon. Avec Network Configuration Manager, cependant, vous pouvez associer chaque règle à un script de correction. Chaque fois qu'une violation est identifiée, tout ce que vous auriez à faire est d'exécuter le script correctif prédéfini, et Network Configuration Manager se chargera du reste.

Un changement qui tourne mal

Au fur et à mesure qu'une entreprise grandit, ses besoins grandissent aussi. Pour répondre à ces exigences sans cesse croissantes, les administrateurs réseau doivent apporter quotidiennement des modifications aux configurations des équipements réseau, mais cela peut créer des failles. Ces failles deviennent une porte d'entrée qui peut causer des vulnérabilités, entraînant éventuellement une perte de productivité et une dégradation des performances.

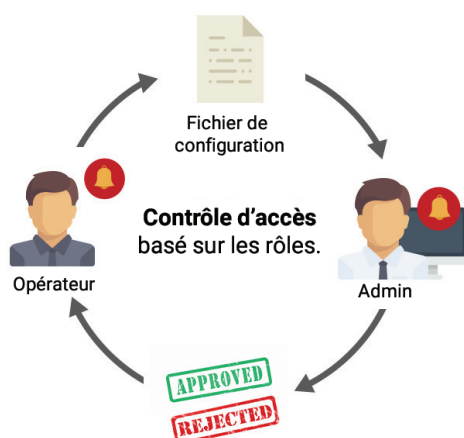
L'une des erreurs courantes qui se produisent pendant la mise en œuvre d'un changement de réseau est l'arrêt des interfaces. La désactivation d'une interface peut rendre inaccessible un groupe de postes sur le réseau, ce qui provoque la déconnexion des utilisateurs. Empêchez les applications critiques de se déconnecter en intégrant la notification des changements, le contrôle d'accès basé sur les rôles et un mécanisme de retour en arrière pour les configurations dans votre workflow de changement. Passons rapidement en revue le fonctionnement de chacun d'entre eux.

Les notifications de changement alertent les administrateurs chaque fois qu'un opérateur a demandé de changer ou de transférer une configuration sur un équipement spécifique du réseau, permettant aux administrateurs d'approuver ou désapprouver ces changements à volonté. Ces notifications permettent également à l'opérateur qui a demandé le changement de recevoir une alerte lorsque ses demandes sont traitées.

Pour les équipements critiques pour lesquels vous voulez empêcher les opérateurs d'apporter des changements irréparables, la meilleure approche serait de mettre en place un mécanisme de retour en arrière (rollback). Un mécanisme de retour en arrière peut être configuré pour ramener le configuration d'un appareil soit à une version précédente, soit à sa version de base configuration. La configuration de référence est souvent le configuration la plus stable et y revenir aide généralement à la rétablir le réseau et réduire des temps d'interruption de productivité.



Dunn & Bradstreet affirme que 59% des entreprises du Fortune 500 connaissent un minimum de 1,6 heure d'arrêt par semaine, ce qui équivaut à un coût hebdomadaire de 896 000 \$ pour la seule perte de main-d'œuvre.



Network Configuration Manager dispose d'une gestion des utilisateurs et l'accès basé sur les rôles vous permet d'ajouter ou de supprimer des utilisateurs, ainsi que de définir leur périmètre d'accès. L'étendue de l'accès doit être définie en fonction du groupe de périphériques avec lequel l'utilisateur interagit habituellement. Par exemple, si un utilisateur ne doit traiter

qu'avec des périphériques Cisco, leur accès peut être limité à ce seul groupe de périphériques. Network Configuration Manager est livré avec des niveaux d'accès prédéfinis qui dictent la portée de chaque utilisateur en définissant les actions autorisées pour ces utilisateurs.

Avec l'accès basé sur les rôles en place, vous recevrez une notification chaque fois qu'un opérateur demande une publication de configuration. Si, à un moment donné, il semble qu'un ensemble approuvé de changements perturbe le fonctionnement de votre réseau, vous pouvez instantanément ramener l'appareil à une configuration de référence. Revenir sur une version fiable d'une configuration d'un périphérique devrait permettre au réseau de se rétablir instantanément, ce qui aidera votre entreprise à assurer la continuité de ses activités.

Perte des modifications apportées dans le réseau

Comme nous l'avons vu précédemment, de nombreuses entreprises ont besoin de changements fréquents dans leurs réseaux pour répondre à leurs besoins croissants. Toute modification apportée à un périphérique s'applique à la configuration en cours d'exécution, ce qui signifie que ces modifications doivent être écrites sur la configuration de démarrage pour éviter que les modifications ne soient effacées en raison d'une perte de courant ou d'un reboot.

Supposons qu'un administrateur réseau crée des politiques qui permettent aux routeurs d'accéder à Internet par l'intermédiaire du fournisseur de services. Lors de la mise à jour de ces configurations, l'administrateur oublie d'écrire ces changements sur le site de démarrage configuration. L'administrateur vient le lendemain pour se rendre compte qu'il y a eu une panne de courant qui a provoqué le redémarrage des périphériques. Cette panne a entraîné la perte des changements et plusieurs utilisateurs ont connu des temps d'arrêt en raison de la perte de connectivité. Si l'administrateur avait synchronisé ces démarrages et exécuté les configurations immédiatement après leur mise en œuvre, il aurait pu conserver tous les changements après la panne de courant et éviter tout temps d'arrêt.



Selon une étude de l'Université de Californie, Irvine, il faut souvent en moyenne 23 minutes pour se refocaliser et se remettre les idées en place après une interruption.

Le processus de synchronisation de configurations est rendu beaucoup plus simple avec Network Configuration Manager. Network Configuration Manager vous donne un aperçu de tous les périphériques de votre réseau qui n'ont pas leur configurations de démarrage et fonctionnement synchronisé. Vous pouvez choisir de consulter un rapport pour voir tous les appareils qui ont un conflit ou d'afficher l'état de chaque appareil dans la liste d'inventaire. Non seulement la liste d'inventaire vous donne des informations sur les appareils qui ont une configuration conflictuelle mais elle vous permet également de synchroniser les configurations. Les synchronisations peuvent également être programmées à partir de l'inventaire pour se produire une fois par mois, par semaine, par jour ou une seule fois.

Une défaillance matérielle

Bien que nous ayons vu comment les changements de configuration peuvent perturber un réseau, il est tout aussi important d'examiner certains aspects matériels clés des périphériques réseau. Un appareil devenu obsolète peut causer autant de dommages qu'un changement de configuration défectueux ou une violation de conformité. La fin du support, la fin de la vente et la fin de la vie utile sont quelques-uns des facteurs qu'un administrateur réseau doit sérieusement prendre en compte lorsqu'il doit gérer ses équipements réseau. Mais sur un réseau qui comprend des centaines de périphériques, il est extrêmement difficile pour un administrateur de garder une trace de ces informations.

Fin du support (End of support / EOS)	Fin de commercialisation (End of sale / EOS)	Fin de vie End of life (EOL)
◆ La fin du support est quand l'assistance technique pour le produit est stoppé d'un constructeur. ◆ L'utilisation de périphériques non pris en charge met un réseau en danger en raison de l'absence de nouvelles mises à jour de sécurité. ◆ Un administrateur peut parfois choisir d'acheter un support étendu, mais cela coûte cher dans la plupart des cas.	◆ La fin de la vente est le moment où un vendeur cesse de vendre un produit. ◆ Les pièces de rechange continuent souvent d'être vendues, de sorte que l'utilisation de tels appareils est fréquente. ◆ Ces appareils peuvent également être achetés auprès de tiers, mais cela comporte le risque d'être vendus défectueux ou contrefaits.	◆ La fin de vie est le moment où un produit a atteint la fin de sa durée de vie utile. ◆ Ces équipements sont généralement obsolètes, il est donc fortement déconseillé de les utiliser. ◆ Les administrateurs doivent mettre ces dispositifs hors service avant qu'ils ne puissent causer des problèmes de sécurité ou de performance.

Network Configuration Manager est livré avec des rapports EOL/EOS intégrés qu'un administrateur peut utiliser à la fois pour créer des documents et pour des audits. Network Configuration Manager fait correspondre les SysOIDs avec les dates données par chaque fournisseur et remplit automatiquement les rapports avec les dates EOL/EOS de chaque appareil. Si les rapports ne comportent pas les dates d'un périphérique, un administrateur peut demander une mise à jour de fin de vie, de fin de support ou de fin de vente à l'équipe de support Network Configuration Manager.



Selon un livre blanc de Joey Fister, expert en situation d'urgence chez Avaya, "52 % des pannes de réseau sont dues à des pannes matérielles".

Remplacer un périphérique en cas de panne matérielle peut être très simple si l'administrateur dispose d'un référentiel de sauvegardes de périphériques. Avec Network Configuration Manager, la prise en charge des sauvegardes de périphériques est beaucoup plus simple. Vous pouvez effectuer des sauvegardes manuelles et planifiées avec Network Configuration Manager. Une fois que vous aurez créé un référentiel de sauvegardes pour tous les configurations de vos périphériques, vous serez en toute confiance pour remplacer un ancien périphérique par un nouveau. Chaque fois que vous avez besoin de mettre en ligne un nouveau fichier de configuration sur un appareil, vous pouvez en choisir un dans la base de données. De plus, l'option de sauvegarde n'est pas limitée aux fichiers de configurations, vous pouvez choisir de sauvegarder des bases de données entières avec Network Configuration Manager.

Se remettre d'une défaillance du réseau

Cela dit, les catastrophes sont parfois inévitables. Il est tout aussi important d'être prêt à résoudre une catastrophe que d'en prévenir une. C'est pourquoi chaque entreprise, quelle que soit sa taille ou son secteur d'activité, doit disposer d'un plan de reprise d'activité (PRA) efficient. Un plan de reprise après sinistre bien organisé doit comprendre des mécanismes de reprise et une sécurité accrue des dispositifs pour assurer la continuité des opérations. Toute application responsable de l'exécution réussie de votre plan doit être en mesure de prévenir, de prévoir et d'atténuer les catastrophes. Network Configuration Manager est l'un de ces outils, car il adopte une approche holistique pour s'assurer que votre réseau est bien protégé et reste résilient face aux désastres du réseau. Ne prenez aucun risque avec votre réseau - préparez dès maintenant un plan de reprise après sinistre réseau à toute épreuve.

Intéressé à apprendre comment les appliquer à votre réseau ? [Inscrivez-vous ici](#) et recevez une démo gratuite de Network Configuration Manager de nos experts techniques.

Faites l'expérience pratique d'un outil efficace de gestion des désastres en réseau. [Téléchargez Network Configuration Manager](#) avec une licence d'essai entièrement fonctionnelle.

Nous contacter :

📄 www.pgsoftware.fr

✉ commercial@pgsoftware.fr

☎ +33 2 51 39 00 92