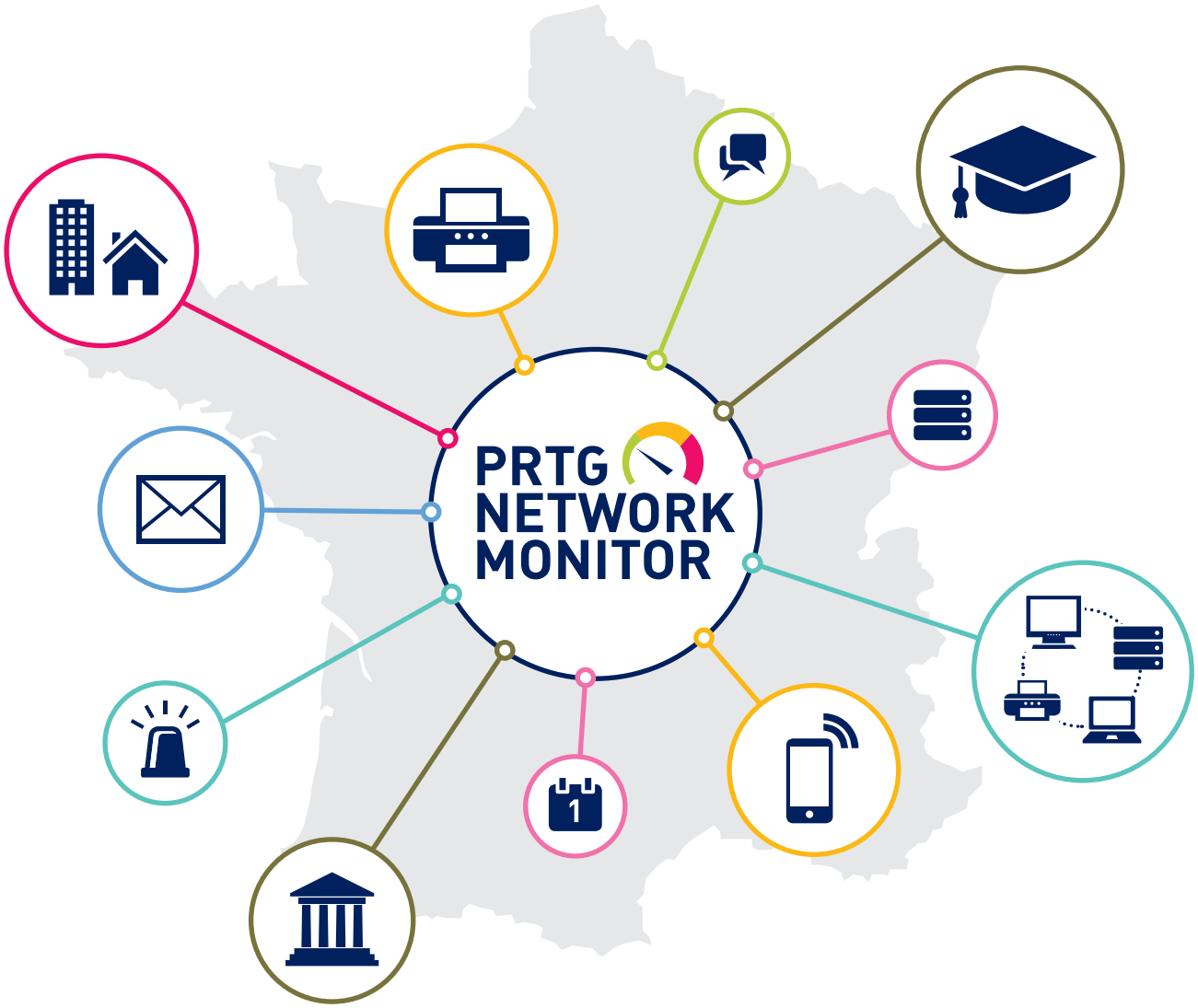
PAESSLER
THE NETWORK MONITORING COMPANY

FOCUS SUR LES ORGANISMES PUBLICS




# Relever le défi de la surveillance réseau au sein des organismes publics

PRTG NETWORK MONITOR

Par Dirk Paessler, fondateur et directeur général de Paessler AG,
éditeur du logiciel de surveillance réseau PRTG

**LE RÉSEAU INFORMATIQUE DE LA VILLE DE SAINTES SOUS HAUTE SURVEILLANCE !**

« Nous sommes très satisfait des fonctionnalités qu'offre la solution de Paessler et en particulier de sa disponibilité 24/24, de la fiabilité de l'application ainsi que la possibilité d'avoir « un historique » des défaillances, la vue d'ensemble et les cartes. »

Pierre-Marc Lis, DSIT de la Communauté d'agglomération de Saintes

Les organismes publics reposent sur une infrastructure informatique pleinement opérationnelle pour mener à bien leurs activités quotidiennes. A l'instar des entreprises du secteur privé, la disponibilité et la performance du réseau doivent être garanties à tout moment, l'apparition de goulots d'étranglement ou de pannes pouvant entraîner de graves conséquences. De plus, les administrations sont confrontées bien souvent à des problématiques spécifiques que ne connaît pas le secteur privé. Il est donc essentiel qu'elles puissent s'appuyer sur un administrateur et un système informatique capables de détecter et de gérer l'ensemble de ces problématiques.

Aujourd'hui, les sites distants sont devenus la règle et ne constituent plus une exception. Agences, multiplicité des sites, centres de données distants doivent tous être intégrés au sein d'un système informatique centralisé. Les réseaux des administrations se construisent bien souvent sur de longues périodes ; ils se caractérisent habituellement par une grande hétérogénéité et s'appuient sur des appareils et des équipements provenant de différents fabricants. D'anciens appareils côtoient souvent des équipements modernes et peuvent varier d'un site à l'autre. Des logiciels et des applications spécifiques sont en outre utilisés par un nombre généralement limité de collaborateurs.

Le stockage centralisé des données permet de gérer efficacement tous ces aspects, sous réserve toutefois de garantir la sécurité et la disponibilité des données à tout moment à partir des sites distants. Pour prévenir toute perturbation importante, l'ensemble des processus et des appareils doit être surveillés en permanence afin de détecter d'éventuels goulots d'étranglement et de les corriger avant qu'ils ne constituent une menace sérieuse. Les informations obtenues permettent d'optimiser les réseaux à long terme et de prévenir la survenue de pannes.

Par ailleurs, les utilisateurs s'attendent de plus en plus à ce que les services en ligne fonctionnent et fournissent des informations 24 heures sur 24. De même que pour les entreprises privées, la productivité augmente si les salariés sont en mesure de travailler depuis n'importe quel lieu et à tout moment.

Le département informatique est tenu de fournir ces services, en garantissant en permanence une sécurité optimale et en respectant les contraintes budgétaires.

# Surveillance centralisée des sites distants

Tous les départements informatiques des organismes publics sont contraints d'assurer l'organisation et la maintenance de sites distants, qu'il s'agisse des bureaux locaux d'une administration ou de centres de données. L'une des approches consiste à déployer sur chaque site des sondes ou « probes » à distance ; ces dernières ne doivent pas être confondues avec les agents, qui sont installés sur chaque appareil afin de les surveiller. Les « probes » collectent les données sur les différents sites, puis les transmettent (cryptées) vers l'installation centrale, chargée d'assurer leur évaluation complète et leur stockage. Ainsi, les frais et les dépenses liés à l'exploitation et à la maintenance restent gérables et l'administrateur système est en mesure de centraliser le contrôle sur l'ensemble du système informatique.

**LA VILLE DE GRENOBLE A CHOISI UN OUTIL DE SURVEILLANCE POUR L'ENSEMBLE DE SON PARC INFORMATIQUE**

« Auparavant, nous effectuions le développement de notre surveillance réseau avec la solution open source Nagios. Nous avons décidé d'en changer car nous trouvions son administration trop fastidieuse, ce qui nous faisait perdre du temps. De plus nous recherchions une solution assez flexible pour avoir le loisir de créer des capteurs personnalisés qui s'adapteraient parfaitement aux différents contextes réseaux que nous devons gérer au quotidien. La simplicité de configuration combinée à la rapidité d'implémentation de PRTG nous ont définitivement convaincus. »

Antoine Meynet, Responsable Sécurité de la DSI de la Ville de Grenoble.

# Une solution unique pour la surveillance d'environnements informatiques hétérogènes

Les réseaux des organismes publics sont divers et hétérogènes. Ils incluent des bureaux locaux, des structures établies, du matériel informatique et des logiciels, ainsi que de la virtualisation. Nombre d'appareils et d'équipements proposent des outils de surveillance spécifiques qui permettent certes des analyses approfondies mais qui ne contribuent guère à fournir une vue d'ensemble de l'infrastructure informatique. Il convient donc de disposer de solutions universelles susceptibles de surveiller à la fois les appareils et les applications des différents fournisseurs, et de garantir un certain niveau de standardisation permettant de maîtriser les coûts et de proposer le niveau de flexibilité requis pour intégrer les différentes solutions existantes.

# Des données hautement sensibles imposent une sécurité maximale, à tous les niveaux

Les autorités locales et les organismes publics ont la charge de gérer les données des citoyens, qui pour une bonne part sont des données sensibles. Les opérateurs d'eau, d'électricité ou de gaz, de même que les services de police ou de pompiers doivent pouvoir intervenir à tout moment. Cela n'est envisageable que dans le cadre d'un environnement informatique fiable et sûr. Les pare-feux, anti-virus et systèmes de back-up constituent des blocks standards au sein d'un concept de sécurité intégré. Il convient toutefois de s'assurer de la fiabilité de fonctionnement de ces différents systèmes. Le pare-feu fonctionne-t-il ? L'antivirus est-il à jour ? Le système de back-up est-il opérationnel ? Une solution de surveillance complète permet de garder un œil sur l'ensemble de ces éléments.

# Traiter les services en ligne

Avec la multiplication du nombre de services publics proposés en ligne, le client/citoyen n'est plus tributaire d'horaires d'ouverture limités. Les employés sont, par ailleurs, en mesure de travailler à l'extérieur de leur bureau. Cette évolution s'accompagne toutefois d'une série d'exigences nouvelles dans le domaine informatique. Par exemple, il ne suffit pas de contrôler les sites web uniquement en termes d'accessibilité ; il convient également de proposer des questionnaires et des téléchargements, et d'assurer le support des systèmes de messagerie et des bases de données. Telle est la condition sine qua non pour permettre aux clients de profiter de cette offre et libérer ainsi les organismes publics de cette charge administrative.

# Une question de coût

Si elle ne doit pas constituer la mission principale des équipes informatiques, la surveillance réseau doit néanmoins permettre de supprimer une bonne partie des tâches routinières quotidiennes de l'administrateur. Pour y parvenir, un premier investissement

s'impose. En effet, autrefois, notamment dans le secteur public, la tendance consistait à recourir à des solutions open source, qui permettaient d'éluder les droits de licence importants associés aux logiciels commerciaux. Pour autant, le choix de l'open source s'accompagnait bien souvent de frais cachés. La mise en œuvre de la solution peut s'avérer sensiblement plus complexe que prévu et il convient d'intégrer également des frais de maintenance récurrents. De plus, les solutions open source exigent bien souvent des ajustements importants pour s'intégrer aux infrastructures existantes. Si un administrateur informatique ou un prestataire de service sous contrat quitte l'organisme public, la solution n'est, bien souvent, plus utilisable. En revanche, les fournisseurs privés proposent des solutions standards qui sont plus faciles à mettre en œuvre et à maintenir.

# Choisir la bonne solution de surveillance

Les défis auxquels sont confrontées les équipes informatiques des organismes publics sont extrêmement variés : hétérogénéité des réseaux, éclatement des sites, responsabilité budgétaire… Les processus internes et le trafic du client dépendent pour une bonne part du haut niveau de disponibilité et de performance du réseau. Pour relever ces défis, les équipes informatiques ont besoin des bonnes informations. Les solutions de surveillance réseau permettent de collecter des informations, mais elles ne répondent toutefois pas toujours aux exigences spécifiques liées aux données sensibles. De fait, il y a lieu d'emblée de procéder à une évaluation exhaustive basée sur les critères suivants :

- Surveillance de différents sites assurée par une solution unique pour un coût et des efforts raisonnables
- Système de surveillance indépendant d'un fournisseur, support pour standards communs
- Adaptabilité aux exigences individuelles, intégration de solutions existantes (API)
- Surveillance fiable de la sécurité et d'autres systèmes essentiels
- Optimisation du réseau à long terme en fonction des données historiques
- Capacité à proposer une surveillance avancée du site web
- Licence à faible coût sans frais ultérieurs importants
- Capacité à surveiller des environnements virtualisés

En intégrant l'ensemble de ces données, la solution de surveillance choisie constituera un facteur décisif à la fois pour la conduite des opérations quotidiennes et pour la planification à long terme, garantissant par là même la stabilité, la sécurité et la rentabilité des organismes publics.

## À PROPOS DE PAESSLER AG

La solution PRTG Network Monitor de Paessler, récompensée de nombreuses fois, est une solution de surveillance unifiée puissante, facile à utiliser et abordable. Il s'agit d'un logiciel hautement flexible et générique, dédié à la surveillance de l'infrastructure informatique et déjà déployé dans des entreprises et organisations de toutes tailles. Plus de 150 000 administrateurs de systèmes informatiques répartis dans plus de 170 pays utilisent PRTG, bénéficiant ainsi d'une tranquillité d'esprit et d'un confort d'utilisation. Fondée en 1997 et basée à Nuremberg en Allemagne, Paessler AG est toujours une société privée et est à la fois membre de la Cisco Solution Partner Program et partenaire de VMware Technology Alliance.

En savoir plus sur Paessler et PRTG : www.fr.paessler.com.

PRTG NETWORK MONITOR