Comment choisir la solution de surveillance réseau adéquate?

Livre Blanc

Auteur: Thomas Timmermann, Directeur Technique des Ventes, Paessler

Publication: Juin 2012

Sommaire

Introduction

Pour que son infrastructure informatique lui donne entière satisfaction, toute entreprise doit pouvoir compter sur un réseau haute performance. Pour maintenir la fluidité des procédures, tous les processus doivent fonctionner de manière fluide, y compris les communications internes et externes entre sites de l'entreprise, ainsi qu'avec les clients et partenaires. Les dysfonctionnements et pannes des processus opérationnels provoquent facilement des pertes de temps et surtout d'argent. Aussi, afin de gérer la disponibilité du réseau informatique, sa performance et la consommation de bande passante, il est vivement recommandé de s'équiper d'un logiciel de surveillance réseau qui veille constamment au bon fonctionnement des processus sur le réseau, effectue des analyses et alerte l'équipe informatique dès qu'une erreur se produit ou que les seuils critiques sont dépassés. Une telle solution de surveillance réseau permet à l'administrateur d'intervenir rapidement, y compris à distance, s'il n'est pas sur place.

Bien entendu, chaque entreprise a ses propres besoins de surveillance réseau. Et comme le marché propose de nombreux outils et solutions différents, il convient de sélectionner avec soin la solution la mieux adaptée. Ce livre blanc fait le point des nombreuses options qu'une solution de surveillance réseau peut proposer et explique quels critères doivent guider la décision.

Pourquoi investir dans la surveillance réseau ?

Une seule et unique solution

Tout le réseau en un clin d'œil

Facile à utiliser

Toujours informé

Planning et optimisation à long terme

Sécurité du fonctionnement

Démarrage rapide

Licence simple et équitable

De plus en plus d'entreprises incluent la surveillance réseau dans leur politique informatique. En effet, la surveillance 24h/24 est rentable à plusieurs égards : elle promet des gains de temps considérables, facilite la planification des ressources pour les administrateurs et contribue à optimiser les performances du réseau de l'entreprise.

Plus de temps pour l'essentiel

Une solution de surveillance se justifie par la détection et le signalement précoces d'erreurs, de dysfonctionnements et de dépassements de seuils, permettant ainsi d'intervenir immédiatement. De plus, l'équipe informatique n'a plus besoin de surveiller constamment l'ensemble des composants du réseau, serveurs, postes de travail, applications, trafic, etc. Ainsi, le système de surveillance fait doublement gagner du temps, que l'administrateur peut consacrer judicieusement à d'autres tâches. Ce que confirme un sondage récent des clients de Paessler AG : 90 % des 724 clients interrogés ont indiqué que leur solution de surveillance réseau PRTG Network Monitor leur fait gagner énormément de temps ; 43 % disent même gagner trois heures ouvrées par semaine.

Sécurité renforcée

Une solution de surveillance contribue à renforcer considérablement la sécurité d'un réseau. Si la solution signale une hausse brutale de la consommation de capacité de traitement ou si le trafic diffère soudainement de la norme, le personnel informatique peut en déduire la présence d'un programme malveillant ou l'existence d'une attaque de phishing. Il est aisé d'intégrer des logiciels de surveillance réseau aux pratiques de sécurité préexistantes (antivirus, pare-feu, etc.) pour renforcer la sécurité de l'entreprise.

2.3. Contrôle accru

Les solutions de surveillance réseau confèrent au personnel informatique plus de contrôle sur leur domaine de responsabilité via la surveillance complète de toute l'infrastructure réseau et le déclenchement immédiat d'alertes. L'équipe informatique maintient le réseau sous observation constante et obtient des informations détaillées sur les processus en cours d'exécution et l'utilisation des différentes ressources. Les informations d'état détaillées sont toutes consultables à tout moment. Comme plusieurs solutions proposent l'accès à distance ou des applications Smartphone, l'administrateur peut continuer à gérer le réseau où qu'il soit. Cela réduit tous les facteurs stress du service informatique qui, en l'absence d'alerte, peut considérer que tout fonctionne normalement.

Identification des potentiels d'optimisation

Il est possible de dégager des tendances fiables de la multitude de données collectées par les logiciels de surveillance réseau. Le personnel informatique dispose ainsi d'un meilleur point de vue sur le réseau pour identifier des potentiels d'optimisation et les concrétiser au plus tôt. Par exemple, le fait de connaître l'utilisation faite de la bande passante permet de mieux prévoir l'attribution systématique des ressources ; ce qui est d'autant plus important pour les projets de virtualisation. Quant à l'administrateur, ces informations peuvent l'aider à mieux tenir les Engagements de Qualité de Service (SLAs).

En utilisant la solution de surveillance réseau appropriée, les engagements de Qualité de Service (SLA) sont garantis.

Economies financières

Etant donné que les solutions de surveillance réseau professionnelles et ultra fonctionnelles sont commercialisées à des prix raisonnables, l'investissement est relativement minime pour les services informatiques au regard du fort potentiel de gains de temps et de ressources. De telles solutions les prémunissent aussi des lourdes pertes financières que pourrait occasionner l'identification tardive d'une défaillance. Au moment de choisir une solution, vérifiez la transparence du modèle de licence du fournisseur, à savoir que les fonctions utiles sont bien comprises dans le prix et non facturées séparément comme des suppléments.

Une solution de surveillance réseau professionnelle permet un gain de temps et de ressources.

En signalant les erreurs au plus tôt, les solutions de surveillance réseau permettent d'intervenir rapidement et d'écourter, voire éliminer complètement les temps d'arrêt. Grâce aux analyses de l'actuel état de fonctionnement du réseau, le personnel informatique peut identifier les faiblesses ou pics de consommation et ajuster les ressources en conséquence pour éviter tout ralentissement des processus métier.

Classification des solutions de surveillance réseau

Comme chaque société, chaque réseau est spécifique avec des attentes particulières vis-à-vis du logiciel de surveillance. Pour couvrir autant que possible l'ensemble des besoins, les éditeurs ont multiplié les solutions au point que la grande diversité des options finit par nuire à la visibilité des offres. Malgré tout, on peut considérer qu'il existe quatre grandes catégories de solutions.

Les logiciels Open Source

En général personnalisables et bon marché, mais suscitent des efforts d'implémentation et de configuration plus intenses.

Beaucoup d'entreprises au budget informatique limité s'intéressent aux logiciels Open Source dans l'espoir de se doter rapidement d'une solution bon marché. A première vue, ces systèmes présentent de gros avantages, puisqu'ils sont souvent hautement personnalisables et utilisables sans payer de licence. Mais quand on y regarde de plus près, les inconvénients finissent souvent par dépasser les bénéfices apparents : à commencer par les efforts d'implémentation et de configuration plus intenses que la moyenne, ainsi que la gamme souvent limitée des fonctionnalités proposées. En effet, seules les fonctions basiques sont généralement intégrées d'emblée, qui ne permettent pas d'assurer une surveillance approfondie du réseau. Autre problème fréquent : le manque de support des fournisseurs, au point que ce sont souvent les utilisateurs de la communauté, au mieux des développeurs qui se chargent du support produit, avec le manque de fiabilité que cela suppose, laissant souvent l'utilisateur seul avec ses questions.

Les solutions de surveillance d'entrée de gamme

Leurs fonctionnalités sont certes limitées, mais elles posent les bases élémentaires.

Ceux qui envisagent d'investir sérieusement dans une solution fiable de surveillance réseau peuvent commencer par des solutions d'entrée de gamme bon marché. Leurs fonctionnalités sont certes limitées, mais elles posent les bases élémentaires : surveillance SNMP de la bande passante ou contrôle de disponibilité via Ping. De ce fait, ce type de logiciels convient aux plus petits réseaux ou pour se familiariser avec la surveillance réseau avant d'investir sérieusement. Il faudra ensuite migrer vers une solution de surveillance plus complète et performante.

Les solutions de surveillance dites « spécialisées »

Surveillance ciblée dans des domaines spécialisés comme la consommation de bande passante au moyen de renifleurs de paquets.

C'est dans cette catégorie que l'on trouve les systèmes de surveillance ciblant des portions spécifiques du réseau ; la consommation de bande passante au moyen d'analyseurs de paquets, par exemple. Ces solutions spécialisées sont très performantes dans leur domaine, mais elles ne conviennent pas pour l'ensemble des besoins de surveillance de tout un réseau. Ce sont généralement des sociétés tout aussi spécialisées qui les utilisent, pour la surveillance de réseaux ou câbles hautes performances, souvent en complément d'autres solutions plus généralistes.

Les logiciels de gestion de réseau d'entreprise

Le système de surveillance n'est souvent qu'une brique parmi les différentes solutions de gestion de réseaux d'une entreprise. Cela se traduit par des coûts élevés et une installation compliquée.

Les systèmes de surveillance ne sont souvent qu'une brique parmi les solutions de gestion de réseau d'entreprise bien plus globales. Ces solutions, aux conditions de licence onéreuses et aux conditions d'installation complexes, ne conviennent généralement pas aux entreprises de taille moyenne. De surcroît, comme elles ne sont pas conçues spécifiquement pour la surveillance réseau, elles ne peuvent pas rivaliser avec les solutions de surveillance réseau indépendantes, ni en termes de fonctionnalités, ni de simplicité d'utilisation.

Les solutions de surveillance « tout en un »

La tendance se concentre, les dernières années, vers des solutions de surveillance réseau « tout en un ».

L'importance croissante de la surveillance réseau professionnelle se traduit depuis quelques années par le développement de solutions de surveillance réseau « tout en un ». Celles-ci combinent fonctionnalités de surveillance générales et fonctionnalités spécifiques pour les sous-domaines spécifiques. Par exemple, ces solutions contrôlent les principaux protocoles, comme SNMP, les analyseurs de paquets, les capteurs de décomposition du trafic pour surveiller la bande passante. Elles proposent également un large choix de capteurs et protocoles de surveillance (SQL, FTP, HTTP, Exchange, POP3, serveurs virtuels, etc.). Ce type de produit s'installe souvent facilement et rapidement et est accompagné d'un service de support professionnel et fiable. Autre avantage : la possibilité d'ajuster les solutions à la croissance du réseau, avec des licences évolutives, aux coûts gérables. Les prix varient de 500 à 50 000 Euros voire plus : d'où la nécessité d'analyser les réels besoins de l'entreprise pour éviter de lourds investissements superflus.

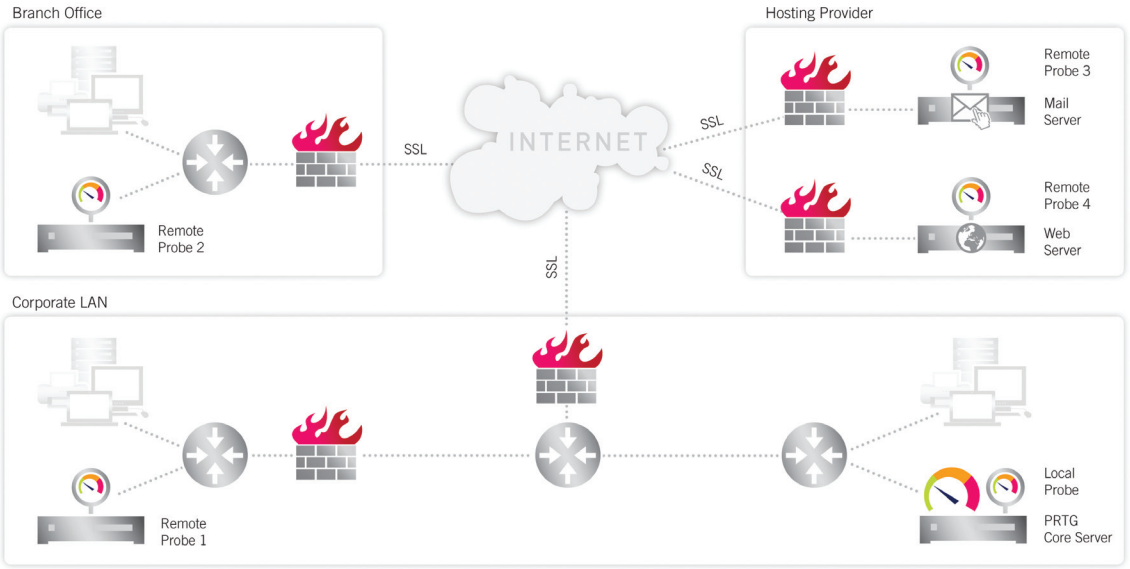

Figure : Une solution conçue pour la surveillance de l'infrastructure informatique globale d'une entreprise répartie sur plusieurs réseaux distribués.

Les critères de sélection de la solution de surveillance réseau adéquate

Outre le coût de la solution, plusieurs facteurs doivent guider votre décision, vis-à-vis notamment de l'infrastructure et des caractéristiques des différentes solutions. Commencez d'abord par répondre aux deux questions suivantes : quelles sont vos attentes vis-à-vis du système choisi et quel sera le contexte d'application de la solution.

Simplification

La première fonction d'un logiciel de surveillance réseau doit être de faire gagner du temps à l'administrateur, qu'il pourra consacrer à d'autres tâches utiles plutôt que de garder l'œil rivé en permanence sur l'infrastructure et l'ensemble des systèmes connectés. Autrement dit, la solution doit fonctionner de façon automatique une fois installée le plus simplement possible, de manière à soulager le personnel informatique plutôt que de lui compliquer la tâche.

Connaissance des besoins

Le choix du bon système de surveillance réseau dépend généralement de la taille du réseau et des périphériques qu'il convient de contrôler, à savoir : serveurs, commutateurs, postes utilisateurs, les connexions entre eux et avec des systèmes distants et Internet. Dans quasi toutes les entreprises, il faut également surveiller le site Web et la messagerie électronique. Concernant le premier, il est important de surveiller la performance globale et les éléments individuels, comme les boutiques en ligne ou les formulaires, de même que les temps de réponse. Les grands groupes mondiaux utilisent des systèmes de surveillance pour mesurer les temps de réponse aux requêtes provenant de différents pays et tenter de les optimiser. Le service informatique utilise de tels logiciels pour maintenir la disponibilité des serveurs d'e-mails POP3 et IMAP. Ils s'en servent aussi pour détecter les éventuelles erreurs de livraison en analysant toute la procédure, depuis l'envoi jusqu'à la réception d'un e-mail test.

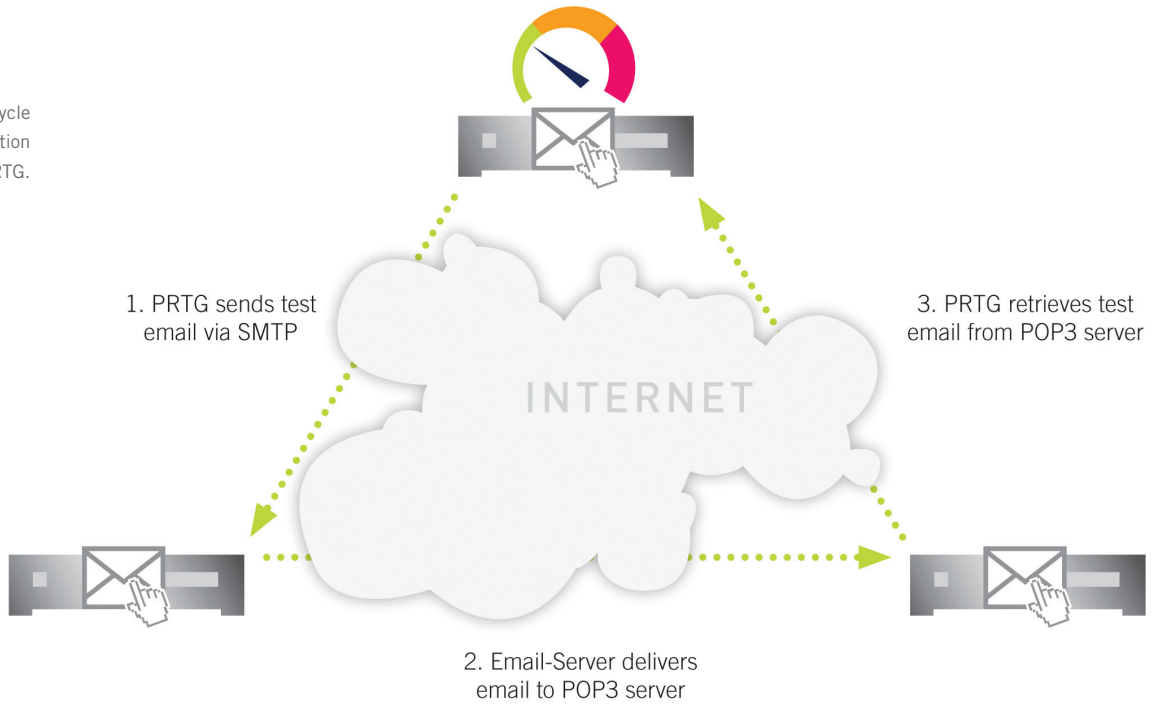

Figure : surveillance du cycle complet d'envoi et de réception d'emails avec PRTG.

Faute de connaissances suffisantes, ceux qui doivent investir dans une solution de surveillance ne pensent pas à toutes les options dont l'application devrait être dotée. De plus, les réseaux sont en croissance constante, ce qui intensifie les besoins de surveillance. Il est donc judicieux d'opter pour une solution qui pourra évoluer avec la demande. Pour lever les incertitudes avant l'achat, demandez à pouvoir tester une version complète en conditions réelles, que vous achèterez si le test s'avère concluant, idéalement en l'état, sans devoir réinstaller une nouvelle version. En cas de problème durant cette phase d'évaluation, vous aurez l'occasion de tester le service de support du fournisseur de manière à entrer en mode opérationnel avec le moins de complications possible.

Figure : la vue Sunburst de PRTG offre un aperçu rapide de l'état du réseau.

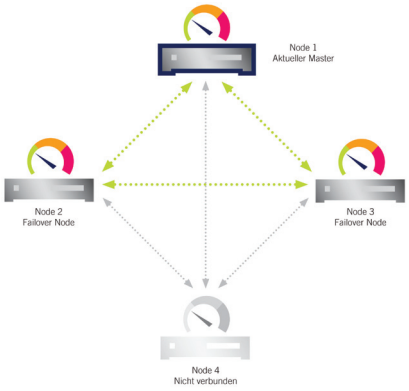

Figure : la fonction de Cluster intégrée de PRTG assure une surveillance sans interruption

Impératifs techniques

Toute solution de surveillance doit permettre de suivre la bande passante et la disponibilité et la consommation des ressources. Elle doit prendre en charge les protocoles et technologies les plus courants (WMI, NetFlow, sFlow, jFlow, les renifleurs de paquets et SNMP, par exemple), les réseaux étant souvent des environnements informatiques extrêmement hétérogènes. Ce n'est qu'en couvrant les protocoles les plus courants que l'on peut espérer obtenir une surveillance suffisamment globale. Vérifiez également que la solution propose la surveillance à distance de multiples implantations ou réseaux distribués. Parfois, pour bénéficier de cette option, il faut souscrire des licences complémentaires ou des offres de services particulières.

Un bon logiciel de surveillance réseau doit informer l'administrateur des niveaux de disponibilité et de consommation de bande passante sous la forme de graphiques, rapports et listes suffisamment détaillés et explicites. Il est important que toutes les données soient archivées pour que le personnel informatique ait une visibilité dans le temps et puisse identifier des améliorations ou changements en fonction de tendances. C'est la base d'une gestion de réseau professionnelle.

Les alarmes sont essentielles pour soulager l'équipe informatique : elles alertent l'administrateur de l'occurrence d'erreurs, chaque fois que des seuils sont atteints ou franchis, ou encore quand des périphériques réseau tombent en panne.

La plupart des solutions permettent l'adaptation des alarmes aux besoins de l'entreprise de façon à ce que l'administrateur puisse être informé par e-mail, par sms, sur pager, via Syslog ou par requête http ; ou que le problème puisse être rectifié automatiquement au moyen de fichiers exécutables .exe.

Pouvoir compter sur ces alarmes procure un sentiment de sécurité et de confort à l'équipe en charge de ces problématiques. Il doit également être possible de définir des actions consécutives aux alarmes : si, par exemple, une solution signale la panne d'un serveur, mieux vaut que les applications qui en dépendent ne génèrent pas chacune leur propre rapport. On évite ainsi d'être submergé inutilement d'alarmes.

Une fonction de cluster intégrée permet de renforcer la sécurité vis-à-vis du risque de panne du système de surveillance. Elle propose que la surveillance soit exercée par plusieurs instances du logiciel en parallèle. Ainsi, si une ou plusieurs instances tombent en panne, les instances fonctionnelles restantes prennent le relais pour maintenir la surveillance sans interruption. L'utilisateur est protégé du risque de panne du logiciel avec l'assurance que le réseau continuera de fonctionner de façon optimale.

Dans le contexte de l'utilisation croissante du Cloud Computing et des systèmes virtuels, il serait légitime que la solution de surveillance réseau propose des options de surveillance de ces systèmes. Elle devrait prendre en charge différents capteurs conçus spécifiquement pour les environnements virtuels, pour VMWare, Microsoft hyper-V, Parallels Virtuozzo Container ou Amazon Elastic Compute Cloud (EC2), par exemple.

Conditions d'utilisation et services

Il va de soi qu'un service de surveillance réseau doit être simple à utiliser, avec des menus clairs et compréhensibles et un mode de fonctionnement intuitif. L'interface doit être souple et pensée pour l'utilisateur, comme une interface Windows, Web ou mobile. En règle générale, la solution doit reconnaître automatiquement le réseau après installation. Il peut être appréciable qu'elle existe dans la langue de travail de l'utilisateur, mais ce n'est pas une obligation.

Figure : les multiples interfaces utilisateurs permettent à la fois un accès direct et à distance.

Les administrateurs amenés à travailler avec des tableaux et des rapports apprécient de pouvoir personnaliser les structures et la composition pour les adapter à leurs besoins spécifiques, pour accéder plus rapidement aux résultats des analyses les plus fréquentes par exemple. Dans la plupart des cas, la solution doit permettre de regrouper des terminaux individuels pour donner un aperçu plus lisible du réseau. Certaines solutions incluent des modèles prédéfinis et personnalisables pour obtenir une vue d'ensemble des composants logiciels et matériels. Le personnel informatique a souvent le choix entre les vues de synthèse et détaillées.

Avant de se décider pour un système de surveillance, l'entreprise a intérêt à examiner les conditions générales avec la plus grande attention. Mieux vaut privilégier les fournisseurs dont les coûts sont transparents, avec des modèles de licence simples et structurés. Vérifiez également les conditions de mise à niveau au gré du développement futur du réseau. Enfin, la solution de surveillance sera d'autant plus attractive que le fournisseur propose des services de support et des informations complémentaires, des manuels d'utilisation par exemple, dans la langue choisie.

Synthèse

Une solution de surveillance réseau complète très avantageusement l'infrastructure du réseau en soulageant les membres du service informatique d'une part et, d'autre part, en permettant d'identifier des possibilités d'optimisation, qui resteraient ignorées sinon. Mais seule une solution alignée sur les exigences du réseau donnera son plein potentiel. Par conséquent, plutôt que d'acheter la première solution venue, les entreprises en quête du système parfait devraient prendre le temps de tester et de comparer. Voici une checklist des questions et critères les plus importants à considérer avant d'acheter.

Checklist de sélection du logiciel de surveillance réseau adéquat

- ☑ Quelles sont les fonctions attendues du système de surveillance ? Quelle est la taille actuelle du réseau ? Existe-t-il des projets de développement à prendre en compte dans la planification ? Existe-t-il des options de mise à niveau rendant la solution pérenne ?
- ☑ A-t-on besoin d'une surveillance complète de l'ensemble du réseau ou uniquement de zones spécifiques ?
- ☑ Existe-t-il une version test de la solution de surveillance qui, dans le meilleur des cas, pourrait être adoptée directement à l'issue d'une période de test concluante pour être opérationnelle sans réinstallation ?
- ☑ Quels protocoles et technologies la solution prend-elle en charge pour la surveillance de disponibilité et de la bande passante ? Est-ce suffisant au regard des besoins de l'entreprise ? La surveillance centralisée de plusieurs implantations distribuées est-elle possible ?
- ☑ Quelles données la solution collecte-t-elle ? Comment sont-elles évaluées ? Les graphiques, rapports, etc. sont-ils personnalisables ? La durée d'archivage des données est-elle suffisante pour dégager et analyser des tendances ?
- ☑ En cas d'urgence, comment les personnes responsables sont-elles alertées ? Peut-on configurer les alertes ?
- ☑ La structure de la solution est-elle conviviale ? Le fonctionnement est-il suffisamment intuitif ? Peut-on configurer les paramètres un par un (l'interface utilisateur est-elle personnalisable) ? L'interface est-elle compatible avec le système d'exploitation, le navigateur utilisé, des terminaux mobiles ?
- ☑ La solution est-elle disponible dans la langue choisie ? Le fournisseur propose-t-il des services de support suffisants ? Existe-t-il d'autres sources d'information (manuels d'utilisateur, blogs et/ou forums) ?
- ☑ La politique des prix du fournisseur est-elle transparente ? Les modèles de licence sont-ils adaptés aux besoins de l'entreprise ?

À propos de Paessler AG

La société Paessler, fondée en 1997 et basée à Nuremberg en Allemagne, est spécialisée dans le développement de logiciels de surveillance réseau et d'analyse de serveur Web. La solution Paessler est déjà utilisée à travers le monde par plus de 150.000 administrateurs réseau, opérateurs de site Web, fournisseurs de services Internet et autres professionnels de l'informatique. Des versions gratuites et d'évaluation de tous les produits peuvent être téléchargées sur www.fr.paessler.com.

Paessler AG
Bucher Str. 79a, 90419 Nuremberg, Allemagne
www.fr.paessler.com, info@paessler.com

N° d'identification de T.V.A. : DE 217564187
N° d'identification fiscale : FA Nürnberg 241/120/60894
Immatriculation au Registre du Commerce : Tribunal d'instance (Amtsgericht) Nuremberg, HRB 23757
Comité directeur : Dirk Paessler, Christian Twardawa Président du conseil de surveillance : Dr. Marc Rössel