PAESSLER

LIVRE BLANC

La surveillance réseau des Clouds privés

Livre blanc

PRTG NETWORK MONITOR

Auteurs : Dirk Paessler, CEO de Paessler AG
Gerald Schoch, Rédactrice technique de Paessler AG

Publication : Mai 2011 – Mise à jour : Février 2015

Sommaire

Introduction

Le concept de « Cloud Computing » n'est pas si récent qu'on pourrait le penser. On le retrouve dans de précédentes approches sous les noms « externalisation » et « hébergement sur serveur », mais qui n'ont pas remporté le même succès du fait des performances insuffisantes des processeurs, des coûts matériels prohibitifs et de la lenteur des connexions Internet. Or, en l'état actuel de la technologie, avec le haut débit et les serveurs de plus en plus performants et de moins en moins coûteux, il devient possible de n'exploiter que les services et l'espace de stockage nécessaire, et de les adapter aux besoins. Le recours aux serveurs virtuels des FAI multiplie les opportunités d'économies financières, de gains de performances et de renforcement de la sécurité des données. L'intérêt de telles solutions Cloud est qu'elles offrent un environnement informatique consolidé, capable d'absorber les fluctuations de la demande et de valoriser les ressources disponibles.

Le concept du Cloud privé

Le concept du Cloud public présente un certain nombre de défis pour les services informatiques d'une entreprise. Les préoccupations concernant la sécurité des données et la crainte de céder le contrôle si un service informatique a l'habitude d'isoler ses systèmes avec des pare-feu et de surveiller l'utilisation de la disponibilité, des performances et de la capacité de son l'infrastructure réseau avec une solution de surveillance approfondie, ces mêmes mesures sont d'autant plus difficile à mettre en œuvre dans le Cloud. Bien sûr, tous les grands fournisseurs de Cloud public offrent des mécanismes de sécurité et des systèmes de contrôle bien pensés. Malgré tout, l'utilisateur de ces services doit toujours s'appuyer sur l'opérateur qui doit lui garantir un accès permanent et maintenir la sécurité de ses données.

La création d'un « Cloud privé » comme alternative au Cloud public est par conséquent une possibilité qui vaut la peine de s'y intéresser. Les Clouds privés permettent aux utilisateurs et aux applications d'accéder aux ressources informatiques nécessaires quand il le faut, tandis que le centre informatique privé ou un serveur privé d'un grand datacenter s'exécute en arrière plan. Tous les services et les ressources utilisés au sein d'un Cloud privé sont limités à des systèmes définis, accessibles aux seuls utilisateurs autorisés et protégés de tout accès extérieur. Les Clouds privés offrent ainsi bon nombre des avantages du Cloud Computing, tout en limitant les risques. Il est en outre possible d'adapter les critères de qualité de performances et de disponibilité d'un Cloud privé et de vérifier l'adhésion à ces critères, ce que ne permettent pas la plupart des Clouds publics.

La surveillance réseau est la base de la planification du Cloud privé

Avant de migrer vers un Cloud privé, tout service informatique doit évaluer les demandes de performance et les fluctuations cycliques de chaque application. Des évaluations approfondies de surveillance réseau peuvent permettre d'analyser les tendances et les pics de demande à long terme, de manière à planifier la disponibilité des ressources en fonction de la demande. Il s'agit d'une étape nécessaire pour garantir la cohérence de fonctionnement des systèmes virtualisés d'un Cloud.

Mais un Cloud privé ne fonctionnera avec fluidité que si les serveurs physiques sont reliés par un réseau ultra fiable et rapide. D'où la nécessité d'analyser en détail toute l'infrastructure réseau avant de configurer un Cloud privé. Ce réseau doit satisfaire les critères de stabilité et de vitesse de transmission, sans quoi il faudra mettre à niveau les équipements ou les connexions réseau. En effet, même des ralentissements minimes de la vitesse de transmission peuvent provoquer des baisses de performance considérables. L'administrateur informatique peut utiliser une solution exhaustive de surveillance réseau en cours de planification d'un Cloud privé. S'il prévoit d'exécuter une application (qui correspond généralement à plusieurs serveurs virtualisés) sur plusieurs serveurs hôtes (« cluster ») dans le Cloud privé, l'application devra utiliser des réseaux SAN (Storage Area Network) comme solution de stockage centrale. D'où l'importance de la surveillance des performances réseau.

LE CLOUD IMPOSE UNE SURVEILLANCE RÉSEAU CONSTANTE

Dans les environnements de terminaux des années 1980, quand un ordinateur central tombait en panne, il pouvait paralyser toute l'entreprise. Le même scénario pourrait se répéter en cas de panne de systèmes au sein d'un environnement en mode Cloud.

Actuellement, alors que nous sommes partis du concept de l'ordinateur mainframe pour ensuite adopter l'informatique et le stockage largement distribués (chaque station de travail ayant son propre PC à part entière), nous revenons finalement au concept d'informatique centralisée. Les données sont hébergées dans le Cloud et les terminaux sont de plus en plus rationalisés (terminaux RDP/Citrix, tablettes, smartphones, etc.). Le nouveau Cloud s'apparente donc à l'ancien concept mainframe de l'informatique centralisée.

La panne d'une seule machine virtuelle d'un environnement Cloud ultra virtualisé peut rapidement bloquer l'accès à 50 ou 100 applications centrales. Les concepts modernes de clustering visent à empêcher de telles pannes, mais s'ils échouent, le problème doit être résolu immédiatement. Dès qu'un serveur hôte lâche, entraînant avec lui un grand nombre de machines virtuelles, ou dès que sa connexion réseau subit des ralentissements ou s'interrompt, ce sont tous les services virtualisés qui dépendent de cet hôte qui en sont instantanément affectés, ce que même les meilleurs concepts de clustering ne parviennent souvent pas à éviter.

L'efficacité d'un Cloud privé, comme de tout autre Cloud, dépend des performances et de la stabilité de l'infrastructure sous-jacente. Les pannes de serveurs physiques ou virtuels, les interruptions de connexion et les routeurs ou commutateurs défaillants risquent de coûter très cher s'ils empêchent le personnel, les processus de production automatisés ou les commerçants en ligne d'accéder aux fonctions informatiques essentielles à leur fonctionnement. Autrement dit, un Cloud privé s'accompagne de tout un lot de nouvelles problématiques pour le personnel en charge de la surveillance réseau.

Pour maintenir l'accès permanent des utilisateurs aux applications métier distantes, il faut absolument surveiller la performance de la connexion au Cloud à tous les niveaux et sous tous les angles. Parallèlement, la fluidité de fonctionnement de tous les systèmes et des connexions au sein du Cloud privé doit être garantie. Et, bien entendu, l'administrateur doit surveiller les interactions entre le Cloud privé et l'environnement informatique des locaux de l'entreprise. Une solution de surveillance réseau appropriée se charge de tout cela au moyen d'un système central ; l'administrateur est ainsi informé immédiatement de l'imminence possible de perturbations de l'environnement informatique privé, sur site et dans le Cloud privé (même si ce dernier est externalisé).

Une des caractéristiques de la surveillance de Cloud privé réside dans le fait que des services de surveillance externes ne peuvent « examiner » le Cloud, celui-ci étant par définition privé. L'opérateur ou le client doit donc prévoir une solution de surveillance de l'intérieur. Ainsi, les équipes informatiques peuvent surveiller le Cloud privé plus directement et précisément qu'en ayant recours à un service du Cloud public. Comme un Cloud privé autorise l'accès sans restriction si nécessaire, l'administrateur peut surveiller l'état des systèmes qui l'intéressent directement à partir d'une solution de surveillance réseau privée. Cette surveillance peut porter sur chaque machine virtuelle, le serveur hôte VMware et tous les serveurs physiques, pare-feu, connexions réseau, etc.

La surveillance réseau du Cloud privé vue sous deux angles

Afin d'obtenir une surveillance globale du Cloud privé, il est important que la surveillance réseau garde constamment en vue les systèmes, que ce soit du point de vue de l'utilisateur et que du serveur. Regardons par exemple le schéma suivant, représentant la surveillance réseau d'une société qui exploite, à l'intérieur d'un Cloud privé, un important site Internet avec une boutique en ligne :

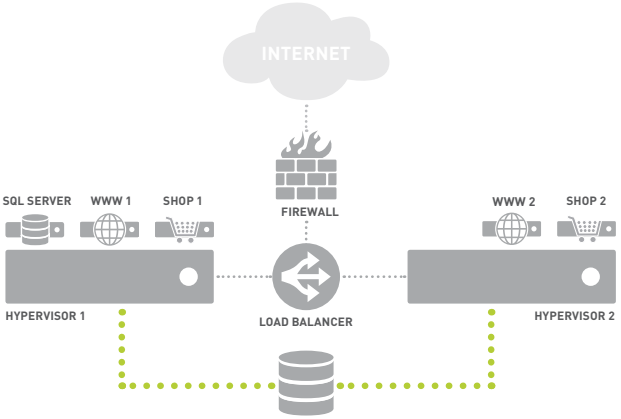


ILLUSTRATION 1:
Schéma de l'hébergement web de la société Paessler AG à l'intérieur d'un Cloud privé

SURVEILLANCE DU POINT DE VUE DE L'UTILISATEUR

La tâche d'un opérateur de site web consiste à veiller à ce que toutes les fonctions soient accessibles en permanence à tous les visiteurs, et cela, quelle que soit le mode de réalisation.

Les questions suivantes peuvent être particulièrement intéressantes à ce point de vue:

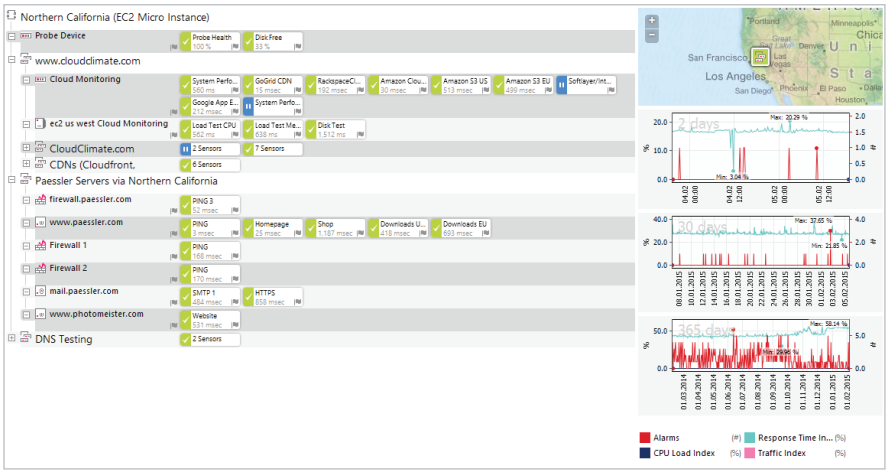
- Votre site web est-il en ligne ?
- Le serveur Web transmet-il les bonnes informations ?
- À quelle vitesse s'effectue le chargement du site ?
- Est-ce que la fonction panier fonctionne ?

Pour trouver réponse à ces questions, il faut que la surveillance réseau se fasse en dehors des serveurs en question ou mieux encore, en dehors des centres informatiques concernés. Par conséquent, l'installation d'une solution de surveillance réseau sur d'autres serveurs de Cloud ou d'autres centres informatiques s'impose. Pour cela, il est crucial que tous les emplacements soient fiables et qu'un cluster de basculement prenne en charge la surveillance afin de garantir une surveillance sans interruption.

Dans l'exemple mentionné ci-dessus, la surveillance à distance de site web devrait par exemple inclure:

- Un pare-feu, un équilibrage de charge HTTP et un envoi de requête ping à un serveur Web
- Des capteurs HTTP /HTTPS pour
  - Le temps de chargement de la surveillance des pages les plus importantes
  - Le temps de chargement de tous les éléments d'une page, y compris CSS, image, flash, etc.
  - La vérification des pages dans le cas ou elles contiennent des mots spécifiques, comme par exemple: "Error"
  - Le calcul du temps de chargement des téléchargements
- La surveillance des transactions HTTP, pour la simulation des processus d'achat
- Les capteurs qui surveillent la période restante de validité du certificat SSL

ILLUSTRATION 2:
Cette capture d'écran affiche plusieurs capteurs PRTG. Ceux-ci sont utilisés pour la surveillance du point de vue de l'utilisateur.



Si l'un de ces capteurs détecte un problème, la solution de surveillance réseau enverra une notification à l'administrateur. A ce stade, il est recommandé d'installer une surveillance réseau basée sur les règles. Par exemple, si le capteur ping d'un pare-feu est en état de delais d'attente, PRTG Network Monitor offre la possibilité de suspendre tous les autres capteurs pour éviter un flot de notifications, puisque dans ce cas, la connexion au Cloud privé est manifestement entièrement déconnectée.

SURVEILLANCE DU POINT DE VUE DU SERVEUR

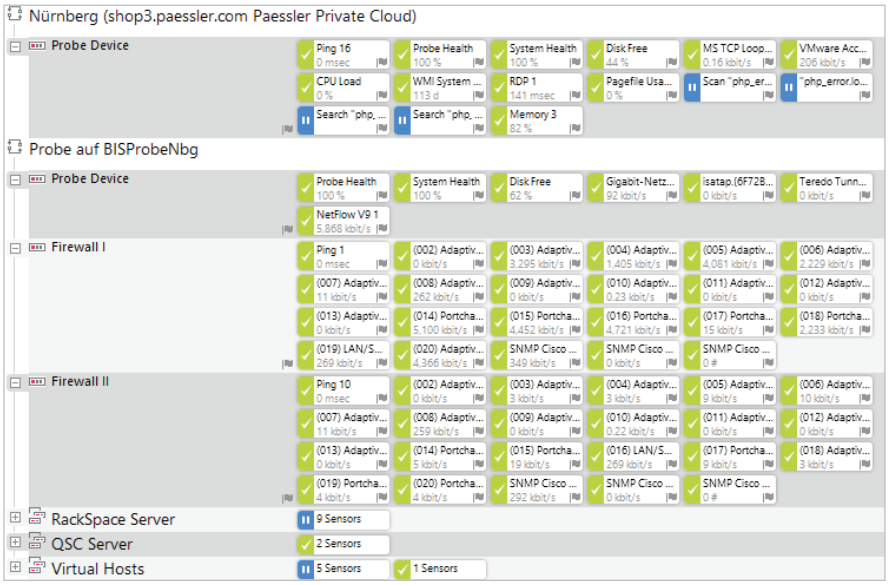
Voici quelques questions déterminantes pour la surveillance de serveurs (virtuels) fonctionnant dans le Cloud privé :

- Est-ce que le serveur virtuel fonctionne parfaitement ?
- Est-ce que la réplication des données internes et le travail d'équilibrage fonctionnent correctement?
- Quel est le niveau d'utilisation du processeur et la consommation de la mémoire ?
- Est-ce qu'il y a assez d'espace de stockage disponible?
- Est-ce que les serveurs de messagerie et DNS fonctionnent parfaitement ?

Avec une surveillance réseau externe, il n'existe pas de réponse à ces questions. Le logiciel de surveillance doit fonctionner sur le serveur ou l'outil de surveillance doit offrir la possibilité de surveiller le serveur à l'aide de sondes distantes (Remote Probes). Ces sondes peuvent par ex. surveiller les paramètres suivants qui se trouvent sur chaque serveur (virtuel) fonctionnant dans le Cloud privé, ainsi que sur les serveurs hôte:

- Utilisation du processeur
- Utilisation de la mémoire (fichiers de page, fichier d'échange, erreurs de page, etc.)
- Trafic réseau
- Accès du disque dur, espace libre sur le disque et temps de lecture / écriture au cours de l'accès au disque
- Paramètres du système de bas niveau (p.ex.: longueur des files d'attente du processeur, commutateurs de contexte)
- Temps de réponse du serveur Web (http)

ILLUSTRATION 3:
Cette capture d'écran affiche la majorité des capteurs PRTG surveillant le système productif du point de vue du serveur.



Les processus les plus critiques, comme les serveurs SQL ou Web, sont souvent surveillés individuellement, en particulier pour l'utilisation du processeur et de la mémoire. De plus, l'état du pare-feu (utilisation de la bande passante, de l'UC) peut aussi être surveillé. Et dès que l'une des variables mesurées dépasse les seuils prédéfinis (par ex. si l'utilisation du processeur est supérieure à 95 % pendant plus de 2 ou 5 minutes), la solution de surveillance en informe immédiatement l'administrateur.

Conclusion

Pour conclure, l'adoption croissante du Cloud Computing génère de nouveaux enjeux à relever pour les administrateurs système. L'efficacité d'un Cloud privé, comme de tout autre Cloud, dépend des performances et de la stabilité de l'infrastructure sous-jacente. Autrement dit, au stade de la planification d'un Cloud, le personnel informatique doit examiner les besoins de capacité de chaque application de façon à dimensionner les ressources qui permettront de satisfaire la demande. La connexion au Cloud doit aussi faire l'objet d'une surveillance constante, car l'utilisateur doit pouvoir accéder en permanence à toutes les applications. Parallèlement, la fluidité de fonctionnement de tous les systèmes et des connexions au sein du Cloud privé doit être garantie. Une solution de surveillance réseau doit donc surveiller tous les services et toutes les ressources sous tous les angles. C'est ainsi que l'on maintient la pleine disponibilité des systèmes et que la planification à long terme, fondée sur les données de surveillance, permet d'éviter tout risque de surcharge.

À PROPOS DE PAESSLER AG

Depuis longtemps, Paessler AG est le leader dans le domaine de la surveillance réseau. La société développe des logiciels de haute performance à des prix abordables et faciles à utiliser. Quelque soit la taille de l'entreprise (bureau à domicile (SOHO), TPE, PME, multinationales), les logiciels de Paessler apportent à la fois tranquillité, confiance et confort dont les services informatiques ont besoin. Grâce à la renommée de ses produits, Paessler dont le siège se trouve à Nuremberg (Allemagne), a déjà en charge plus de 150.000 installations à travers le monde. Fondée en 1997, Paessler AG est toujours une société privée et est à la fois membre de la Cisco Solution Partner Program et aussi partenaire de VMware Technology Alliance.

Des versions gratuites et d'évaluation de tous les produits peuvent être téléchargées sur www.fr.paessler.com/prtg/download.

Paessler AGwww.paessler.fr, info@paessler.com