SIMPLY SECURE

G DATA TechPaper #0375

G DATA Network Monitoring

G DATA Software AG | Application Development | 2016

Table des matières

Introduction

L'inter-connectivité du matériel informatique, tel que les postes de travail, serveurs, dispositifs intelligents, imprimantes et autres périphériques, est forte. Le fait que ces appareils soient reliés entre eux dans un réseau amène des déploiements et des stratégies de gestion complexes. Suivre tous ces éléments actifs et les maintenir à niveau est un défi constant. Network Monitoring (monitoring réseau) aide les administrateurs IT à assurer la continuité d'activité d'une entreprise par la surveillance d'une large gamme d'éléments réseau. Les administrateurs assurent une maintenance et une assistance efficace en anticipant les incidents et planifiant plus facilement les déploiements et les upgrades. Network Monitoring permet une gestion des éléments actifs du réseau, l'optimisation des performances et une maintenance plus efficace pour tout type de structure, de la petite à la grande entreprise.

1. Atouts de Network Monitoring

1.1. Disponibilité

La multiplicité des appareils sur le réseau rend difficile l'identification des risques et des problèmes de performance. Network Monitoring permet d'identifier en continu les problèmes de performance, de suivre les tendances d'utilisation et d'anticiper les problèmes de disponibilités. Par l'utilisation des journaux, les points faibles du réseau peuvent être optimisés avant que la charge n'affecte la performance ou n'engendre une coupure. Quand les utilisateurs rapportent des problèmes avec la base de données, le système CRM ou la boutique en ligne, les journaux d'erreurs sont également très utiles.

1.2. Migration et extension

Network Monitoring aide dans les développements d'infrastructure tels qu'une migration ou une extension du réseau. En connaissant la topologie du réseau, les administrateurs identifient les composants de l'infrastructure qui nécessitent des améliorations et s'assurent que le réseau a tous les prérequis pour le déploiement.

En journalisant le fonctionnement sur une longue période, les administrateurs peuvent gagner en visibilité sur les niveaux de performance. Les sondes peuvent prendre en charge les temps de réponse de l'infrastructure ou d'applications, l'utilisation, le débit ou les capacités. Ils peuvent alors servir comme indicateurs de référence lors de la planification d'une nouvelle infrastructure pour des scénarios de migration ou d'extension afin de prendre des décisions selon des critères d'évolutivité et de disponibilité.

1.3. Conformité

Network Monitoring peut être configuré pour enregistrer une large gamme de données. Il est donc adapté à des fins d'audit et de conformité. Il ne permet pas uniquement de suivre les données d'usage des appareils dans l'infrastructure réseau, il peut également contrôler des configurations par défaut et détecter les changements de configurations. Cela permet aux entreprises de préparer leur infrastructure pour des certifications et être sûres qu'elle ne déroge pas aux règles de conformité sur lesquelles est basée l'infrastructure.

1.4. Sécurité

Network Monitoring aide à détecter les signes d'activités douteuses, comme une charge inhabituelle qui peut indiquer une attaque de déni de services (DoS). Les appareils infectés peuvent générer des charges CPU ou des services inhabituels. L'utilisation de la mémoire, l'apparition de processus ou une augmentation de trafic peuvent aussi être des signes d'infection. Combiné avec une solution de gestion des correctifs sur les endpoints, Network monitoring aide les administrateurs à détecter et atténuer rapidement et facilement les vulnérabilités.

1.5. Cloud et virtualisation

Dans des gestions d'infrastructure en Cloud, de serveurs virtuels ou d'autres scénarios multipartites, Network monitoring peut aider à maintenir un modèle stable. Network Monitoring aide à estimer les besoins et à surveiller les performances de toutes les applications et services sur le réseau. La solution aide également à préparer la virtualisation de serveurs physiques en mesurant leur accès lecture/écriture, le trafic réseau, l'utilisation CPU et d'autres statistiques relatives à la performance. Enfin, Network monitoring peut également être utilisé comme outil de surveillance dans le cadre d'accord sur des niveaux de services garantis ou encore des cas de facturation à l'utilisation.

2. Choisir une solution de Network Monitoring

Les entreprises de toute taille ont déjà découvert la valeur ajoutée d'un Network Monitoring intégré à leur processus de gestion IT. Le marché sur ces solutions augmente en conséquence : le chiffre d'affaires total en 2012 a été estimé à 2,2 milliards de dollars et devrait arriver à 4,5 milliards de dollars en 2017, avec un taux de croissance annuel de 15,2%[1]. Car il existe une multitude de solutions disponibles, il est important de s'informer avant toute acquisition.

2.1. Fonctionnalités

Le premier point à considérer dans la qualification d'une solution de Network Monitoring est la prise en charge des protocoles de communication. La solution doit être capable d'interpréter les données d'un maximum d'appareils du réseau. Dresser un inventaire de l'infrastructure du réseau aide à trouver quels protocoles doivent être déployés.

Les capacités de journalisation des données sont aussi un point important. Pour l'analyse des tendances, la solution doit pouvoir sauvegarder des données sur une longue période et être capable de produire des rapports de tendances et des graphiques.

Dans le cadre de la mise en place d'un système de réponse sur incident, la solution doit permettre aux administrateurs de déterminer des valeurs seuil de déclenchement d'alertes.

Pour finir, et afin de faciliter la gestion de l'outil, les fonctionnalités doivent être disponibles dans une interface unifiée, à travers un tableau de bord clair donnant rapidement accès à toutes les informations importantes.

[1] Frost & Sullivan: Network and Application Performance Management Market (2012).

2.2. Retour sur investissement

Le coût d'une solution de Network Monitoring doit, bien entendu, être étudié. Mais un retour sur investissement est aussi à prendre en compte.
Les gains les plus évidents sont la prévention de pertes d'activités dues à des problèmes techniques et des coupures réseau. La disponibilité d'un serveur web ou d'un serveur de base de données est cruciale dans l'activité d'une entreprise.
En utilisant Network Monitoring, le nombre de coupures dans l'infrastructure peut être réduit par des actions correctives avant que le réseau ne ralentisse ou ne s'arrête.
Dans le cadre d'une panne matérielle soudaine, les alertes garantissent une réponse rapide de l'équipe de maintenance.

3. G DATA Network Monitoring

G DATA a intégré Network Monitoring dans sa gamme de solutions. Cela permet aux administrateurs de profiter d'une synergie entre la gestion de l'architecture réseau et la sécurité des postes clients.

3.1. Déploiement

Network Monitoring est disponible en tant que module optionnel de toutes les solutions G DATA BUSINESS depuis la version 14.0.

L'architecture de la solution se compose de trois éléments : l'interface d'administration web distante G DATA ActionCenter (accessible sur https://ac.gdata.de), le G DATA ManagementServer (serveur local de mise à jour des solutions G DATA) et les clients G DATA Security (protection antivirale installée sur les postes clients).

En pratique, les clients G DATA Security collectent les informations des sondes, les envoient aux G DATA ManagementServer, qui les synchronise avec l'interface distance G DATA ActionCenter.

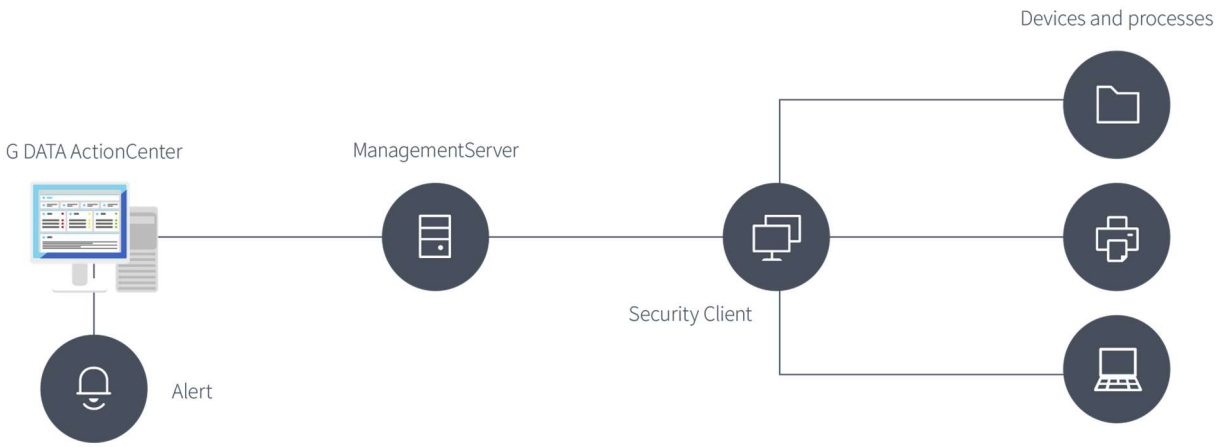

Illustration 1: Architecture de G DATA Network Monitoring

Grâce au client G DATA Security et à la prise en charge de différents protocoles de communication, Network Monitoring dispose d'un large panel de sondes, du matériel aux processus système. Exemple de sondes disponibles :

- Matériel
    - Endpoints et serveurs
        - Disque dur
        - CPU
        - RAM
        - NAS
    - Infrastructure réseau
        - Endpoint et interface serveur réseau
        - Routers
        - Switches
        - Points d'accès
        - Pare-feu
    - Périphériques
        - Imprimantes réseau
- Logiciel
    - Processus et services
        - Systèmes d'exploitation
        - Applications
    - Serveurs
        - Web
        - Base de données
        - Exchange
        - Contrôleur domaine

Pour couvrir ce spectre, plusieurs protocoles sont pris en charge.

Le SNMP (Simple Network Management Protocol) est un standard. Utilisé dans de nombreux appareils réseau, il se caractérise par une structure question-réponse : le serveur de Network Monitoring demande l'état de ses sondes à l'appareil, qui lui répond en retour. Pour ce faire, le protocole SNMP ainsi que les sondes adéquates doivent être activés dans l'appareil. Ceci se réalise par l'interface d'administration de celui-ci.

Deux autres sources d'acquisition de données sont également disponibles : Performance Counters et l'API Windows Management Instrumentation (WMI). Tous deux sont disponibles pour la majorité des agents basés sur Windows.

Des éléments qui ne disposent d'aucun de ces trois protocoles peuvent être contactés en utilisant la commande ping ou via une communication basée sur http.

3.2. Configuration

Network monitoring est configuré et géré grâce à l'interface Web du G DATA ActionCenter https://ac.gdata.de.

Pour commencer, un ou plusieurs modèles de sondes doivent être créés. Un modèle contient un type de monitoring et ses paramètres.

Exemples :

- Contrôler un processus dans Windows
- Contrôler la disponibilité d'un serveur
- Contrôler le niveau d'encre d'une imprimante

Les paramètres de configuration peuvent inclure une valeur seuil. Ceci permet de générer des alertes si la valeur est dépassée ou chute sous ce seuil. Ces alertes sont envoyées sur des boîtes email dont les adresses sont à définir dans les paramètres du modèle

Le modèle créé, il suffit ensuite de l'attribuer à un ou plusieurs éléments du réseau (client Windows, imprimantes, etc.).

Ces éléments sont alors régulièrement contrôlés par la sonde. Les informations sont envoyées au ManagementServer local qui les synchronise avec l'ActionCenter.

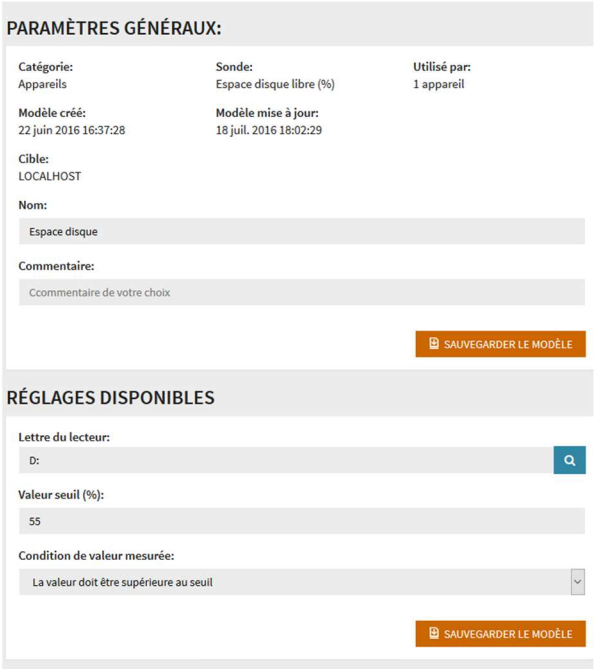

Illustration 2: Modèle

3.3. Analyse

Avec une ou plusieurs sondes créées, les administrateurs peuvent suivre de plusieurs façons les données reportées.

Pour des scénarios qui dépendent de rapports immédiats, les alarmes sont la méthode de notification recommandée. Ils permettent d'avoir un temps de réponse rapide en cas d'urgence. Les alarmes peuvent être actives dans les modèles de sondes et sont valables pour toutes les sondes basées sur ce modèle. Lors de l'activation d'une alarme, il est recommandé de s'assurer que les groupes appropriés d'adresses email ont été définis pour être sûr que le problème soit traité rapidement. Les notifications peuvent être envoyées à une liste de distribution d'adresse mail, telle qu'une équipe d'urgence d'un service informatique.

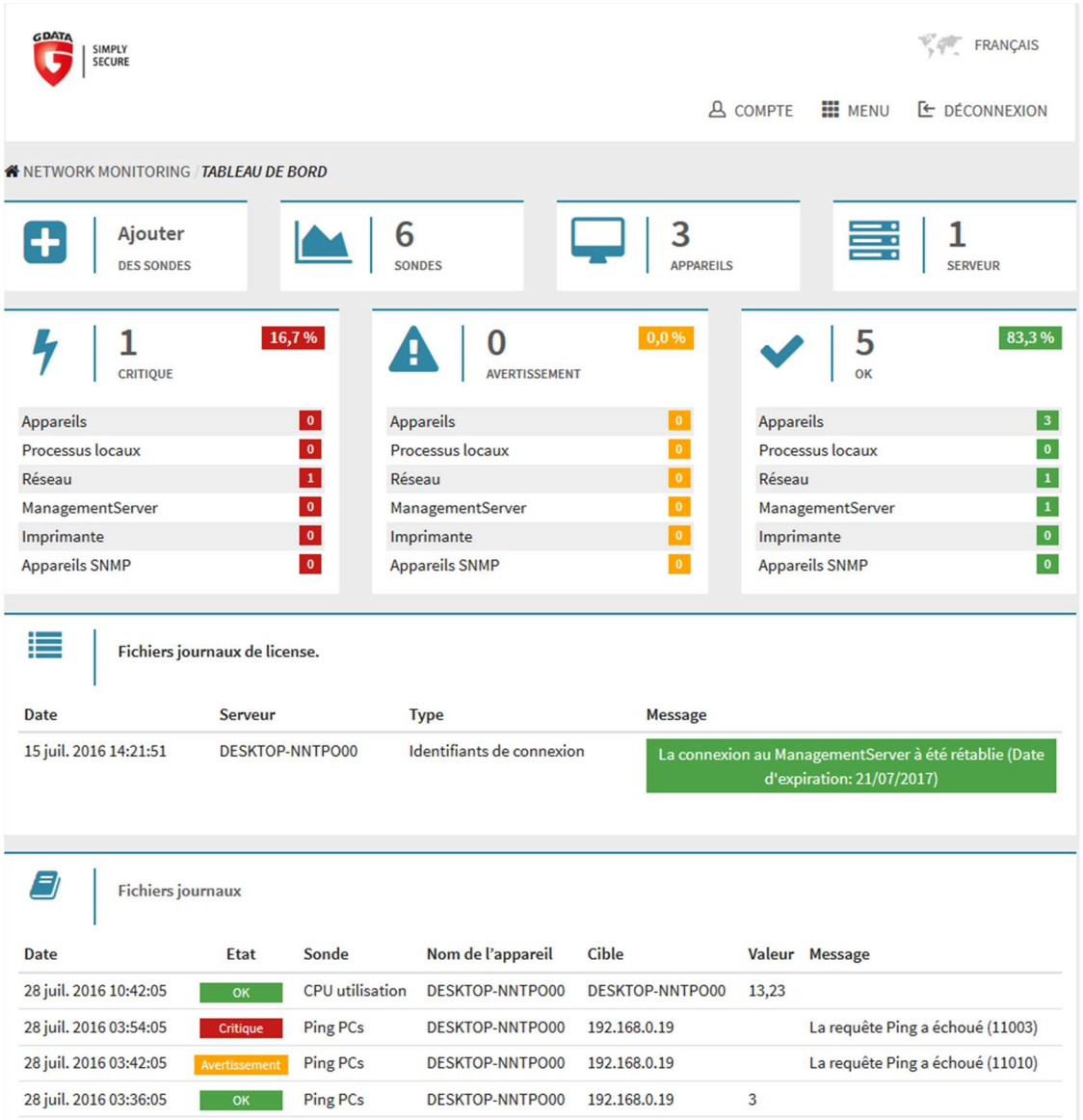

Illustration 3 : Tableau de bord

Les administrateurs n'ont pas à attendre que l'alarme soit envoyée. Le tableau de bord du G DATA ActionCenter avise des informations essentielles sur le statut du réseau. Trois indicateurs de statut affichent les statistiques de contrôle de service par priorité (critique, avertissement, normal). Cela permet aux administrateurs de voir rapidement si une intervention est nécessaire. Des services individuels peuvent être mis en favoris afin de les afficher directement sur le tableau de bord, ce qui est spécialement utile pour les éléments importants ou utilisés fréquemment. Le nombre de ManagementServer associés tout comme le nombre d'appareils sont affichés, ce qui facilite la vue d'ensemble du réseau.

Si une analyse plus détaillée est nécessaire, les pages de sondes individuelles peuvent être utilisées. Chaque page affiche un diagramme, permettant aux administrateurs de repérer des tendances

avant qu'elles n'atteignent le niveau critique. Le diagramme peut être configuré pour afficher des valeurs pour une durée spécifique et utilisé pour pointer les tendances.

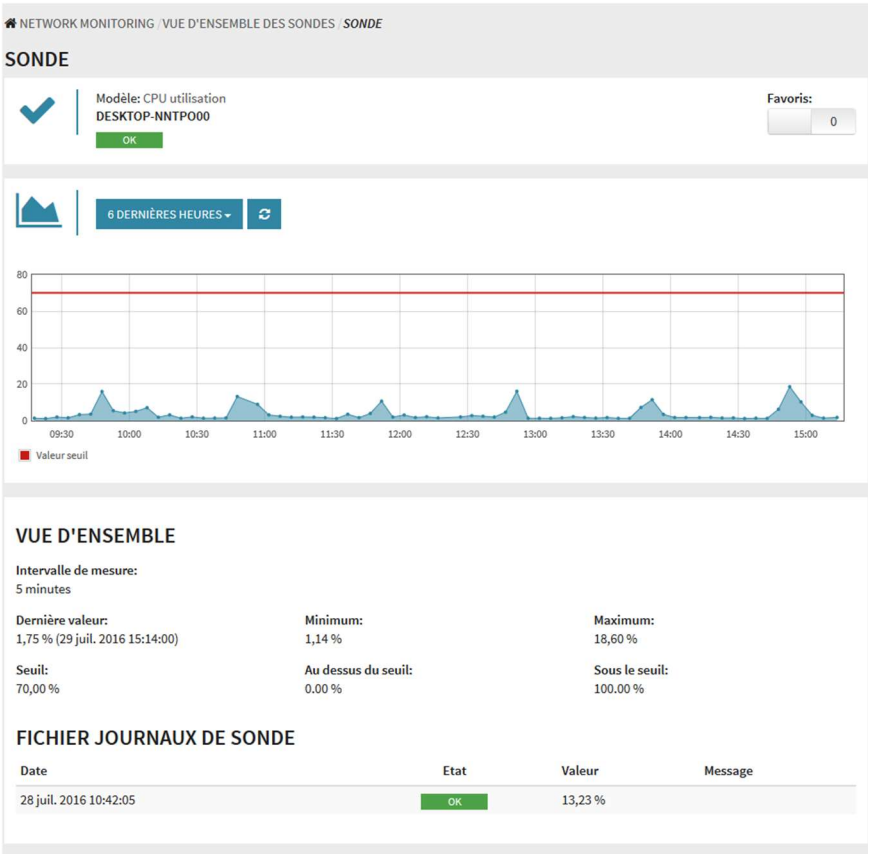

Illustration 4 : Sonde

De multiples scénarios de monitoring sont possibles. Quelques exemples :

- Quand l'usage de mémoire vive d'un appareil affiche une tendance à la hausse avant de descendre soudainement, alors cela peut indiquer un problème d'usage de la mémoire d'un processus spécifique. Pour identifier le problème, les administrateurs peuvent mettre en place d'autres sondes de processus système, ou rechercher un problème matériel.
- En utilisant les journaux, il est aussi possible d'identifier une potentielle surcharge d'une interface réseau. Des alertes peuvent être mises en place en fonction de ces seuils afin d'identifier, par exemple, si l'infrastructure réseau est la cause d'un ralentissement du CRM.

Quel espace disque reste-t-il sur l'espace de sauvegarde ou de partage ? Quel est l'espace de mémoire vive disponible en moyenne sur les postes clients ? La charge processeur du serveur est-elle normale ? Quel est le délai de disponibilité du serveur intranet ? Etc. En combinant les sondes, l'administrateur peut facilement être informé du niveau de criticité de son réseau.

Vous souhaitez en savoir plus sur le monitoring ? Contactez l'équipe G DATA Software France.