Annexe 1 : Le cahier des charges

Le cahier des charges présenté à CSI Systèmes et Réseaux se compose des éléments suivants :

➢ *Périmètre de l'étude et dimensionnement de la configuration*

La partie serveur de cet outil devra être implémenté sur un serveur AIX ou Solaris et devra être capable d'assurer la surveillance de l'environnement défini ci dessous.

Surveillance des serveurs NT

Le client possède 70 serveurs NT à surveiller avec en moyenne :

- 5disques,
- 10 services,
- 1 log avec 5 mots clés
- Fréquence de pooling[1] :60 secondes

Surveillance des serveurs UNIX

Il possède également 100 serveurs UNIX à superviser avec en moyenne :

- 15 Filesystems
- 25 process
- 1 log avec 5 mots clés
- Fréquence de pooling : 60 secondes

Equipements réseaux

Les équipements réseaux à surveiller sont au nombre de 600, pour lesquels :

- 15 demandent un pooling de 15 secondes,
- 125 demandent un pooling de 30 secondes
- et le reste demandant un pooling de 60 secondes

➢ *Expression des besoins*

Pour répondre aux besoins de surveillance du client, l'outil devra réaliser les différentes fonctions nommées ci-dessous. Certaines sont fondamentales (A), d'autres très importantes (B) et certaines moyennement importantes (C).

➢ Remplissage des disques

- Pouvoir fixer un seuil critique A
- Pouvoir fixer un seuil Warning destiné aux responsables. B

➢ Présence des processus

- Définition du nom de processus : A
  - Commençant par xxx
  - Finissant par xxx
  - Contenant la chaîne xxx

[1] Pooling :fréquence de mise à jour.

- Exactement xxx

- Nombre d'occurrence du process : A
  - Au moins N
  - Au plus N
  - Exactement N
  - Entre N et M

- Pouvoir associer un niveau de gravité (Warning, critique) pour chaque alerte. B

➢ **Analyse de fichier Log**

- Recherche de lignes : A
  - Commençant par xxx
  - Finissant par xxx
  - Contenant la chaîne xxx
  - Exactement xxx

- Pouvoir donner un mot clé qui déclenchera l'alerte, et un autre qui arrêtera l'alerte B

➢ **Traitement des trames SNMP**

- Interfaçage avec des équipements particuliers : A
  Baies disque EMC, Equipements réseaux, Surveillance des bastions

➢ **Activité CPU**

- Pouvoir fixer un seuil pendant une durée donnée A
  Ex : 90% pendant 15mn
- Pour les serveurs multiprocesseurs : pouvoir remonter une alerte par CPU et sur la globalité des CPU. C
  Ex :Pouvoir détecter un process qui par en boucle sur un CPU

- Eventuellement, pouvoir fixer 2 seuils : un warning et un critique B
  Ex : Warning à 100% pendant 5mn, Critique à 90% pendant 15mn

➢ **Utilisation de la mémoire**

Pour que cette information soit pertinente, il faut remonter l'utilisation réelle de la mémoire par les process en machine.

- Pouvoir fixer un seuil critique
  A
  Ex :80%

- Pouvoir fixer un seuil de warning, qui passe en critique au bout d'un temps donné
  Ex :warning à 80%, qui passe à critique au bout de 15mn B

- **Utilisation du Swap et/ou pagination**

  - Pouvoir fixer un seuil critique
    B
  - Pouvoir fixer un seuil de warning, qui passe en critique au bout d'un temps donné C

- **API pour surveillance des services et applications**

  - Services NT B
  - Notes B
  - Oracle B
  - Ingres C
  - MQseries B

- **Activité disque**

  - Pouvoir surveiller pour chaque disque B
    - le taux d'activité
    - le débit global
    - le temps d'accès moyen
  - Remonter une alerte si un des disques à une activités supérieure à un seuil pendant une durée donnée B

- **Taille des fichiers logs**

  - Pouvoir déclencher une alerte si la taille d'un fichier log dépasse une certaine valeur B

- **Nombre d'Inode**

  - Pouvoir fixer un seuil critique B

- ***Les fonctions et outils***

- **Centralisation des alertes**
  - Une console log surlaquelle apparaîssent toutes les alertes en cours. Elle doit disparaître lorsque le défaut n'est plus présent.
  - Une vue sur tous les serveurs.

- **Administration des alertes**
  - Outil graphique pour définir et modifier les alertes.
  - Avoir une vue de toutes les alertes.
  - Avoir des statistiques sur les alertes.

- **Sauvegarde des données.**
- **Corrélation d'événements**
  - Pouvoir annuler une remontée d'alerte si une autre alerte est déjà présente.

- **Traitement des alertes**

- Pouvoir mettre un commentaire sur une alerte.
- Associer une consigne sur chaque alerte.
- Suspendre l'alerte pendant une durée.
- Lister les alertes suspendues.
- Associer un signal sonore à une alerte.

- **Pouvoir router une alerte.**
- **Pouvoir associer un calendrier et une plage horaire pour chaque alerte.**
- **Normalisation des messages.**
- **Pouvoir contrôler l'état de la surveillance.**

Activation / Désactivation d'une alerte