

1. NARETO : définition d'indicateurs complexes, reporting et capacity planning

1.1.Présentation

Nareto est un outil qui se place au dessus de Nagios. Nareto est composé de trois modules: un module de suivi en temps réel de l'état de tous les services, un module de reporting et un module d'analyse des alertes. Nareto permet de composer les différents indicateurs configurés complètement librement. Ceci aboutit à l'obtention d'une vue fonctionnelle correspondant exactement au Système d'Information supervisé.

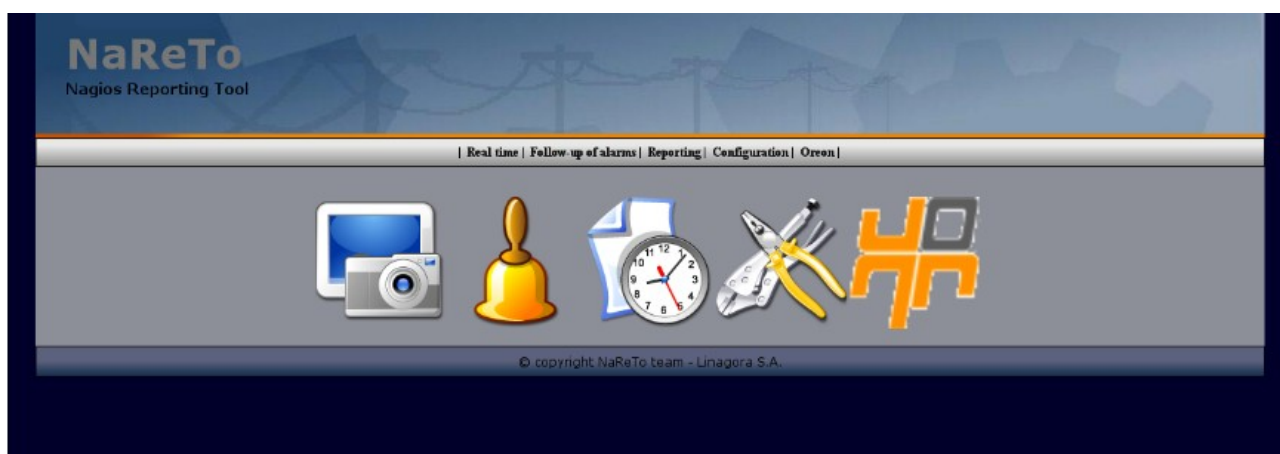


Figure 1 : Page d'accueil

1.2.Vue macro vers le micro

Avec Nareto, on définit un arbre de navigation que l'utilisateur va parcourir. La racine est virtuelle ce qui permet d'avoir plusieurs noeuds au niveau le plus haut (voir image au dessous).

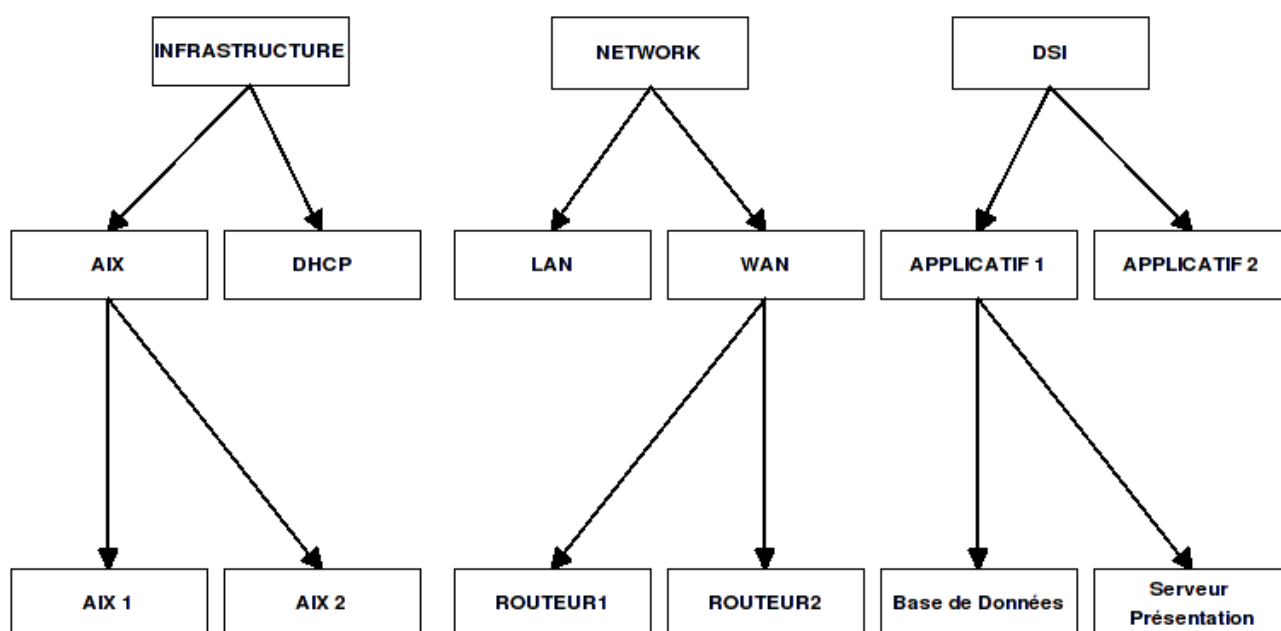


Figure 2 : Exemple d'enchaînement de noeuds

On parcourt les noeuds du niveau le plus haut (la vue fonctionnelle, que l'on appelle en général « domaine ») vers le niveau le plus bas (la vue technique, l'indicateur). Un noeud peut contenir plusieurs noeuds, ce qui correspond à une vue fonctionnelle. Un noeud peut contenir des indicateurs, ce qui correspond à une vue technique.

Il est tout à fait possible qu'un noeud corresponde à un équipement donné (serveur, switch, routeur ou firewall). Ce noeud contiendra donc tous les indicateurs de l'équipement. Si l'on ajoute par la suite un nouvel indicateur à cet équipement, Nareto le prendra en compte automatiquement.

A l'inverse, on peut associer des indicateurs d'équipements différents dans un noeud donné. Ceci permet d'avoir une vue sur un applicatif composé. Par exemple, dans le cas d'applicatif n-tiers séparé sur différents serveurs, il est intéressant d'avoir une vue complète sur l'applicatif entier. Or, les différentes parties étant situées sur différents équipements (serveur de base de données, serveur d'authentification, serveur applicatif) il suffit de créer les indicateurs sur les différents serveurs puis de les agréger dans un noeud qui porte le nom de l'applicatif.

Note : il est tout à fait possible qu'un indicateur donné soit présent dans deux noeuds différents, on peut donc avoir les deux visions en même temps, sans que cela ne pose aucun problème

1.3. Vue différente selon les profils utilisateurs

Un profil utilisateur représente un groupe d'utilisateurs avec des droits sur des noeuds donnés. On peut définir autant de groupes d'utilisateurs qu'on le souhaite. Cette notion de profils permet de limiter la vue sur certains noeuds uniquement. Dans le cas d'équipes d'administration différentes pour un Système

d'information, l'équipe gérant le réseau n'a pas forcément besoin de connaître l'état des différents serveurs. De même, le profil DSI n'a pas besoin de savoir quels éléments précis ne fonctionnent pas : savoir que c'est le disque, le CPU, l'applicatif de base de données, le système de fichier ou l'applicatif web qui connaît un problème leur importe peu. Ce qu'il souhaite, c'est de savoir si cela fonctionne ou pas en fonction des domaines définis. Pour cela, il suffit de créer plusieurs domaines différents. Un domaine est réservé à une vue de très haut niveau où l'information est : « l'ensemble de l'applicatif fonctionne » (vue fonctionnelle). Un domaine est réservé à l'équipe technique qui aura une vue sur tous les indicateurs de ce domaine (vue technique).

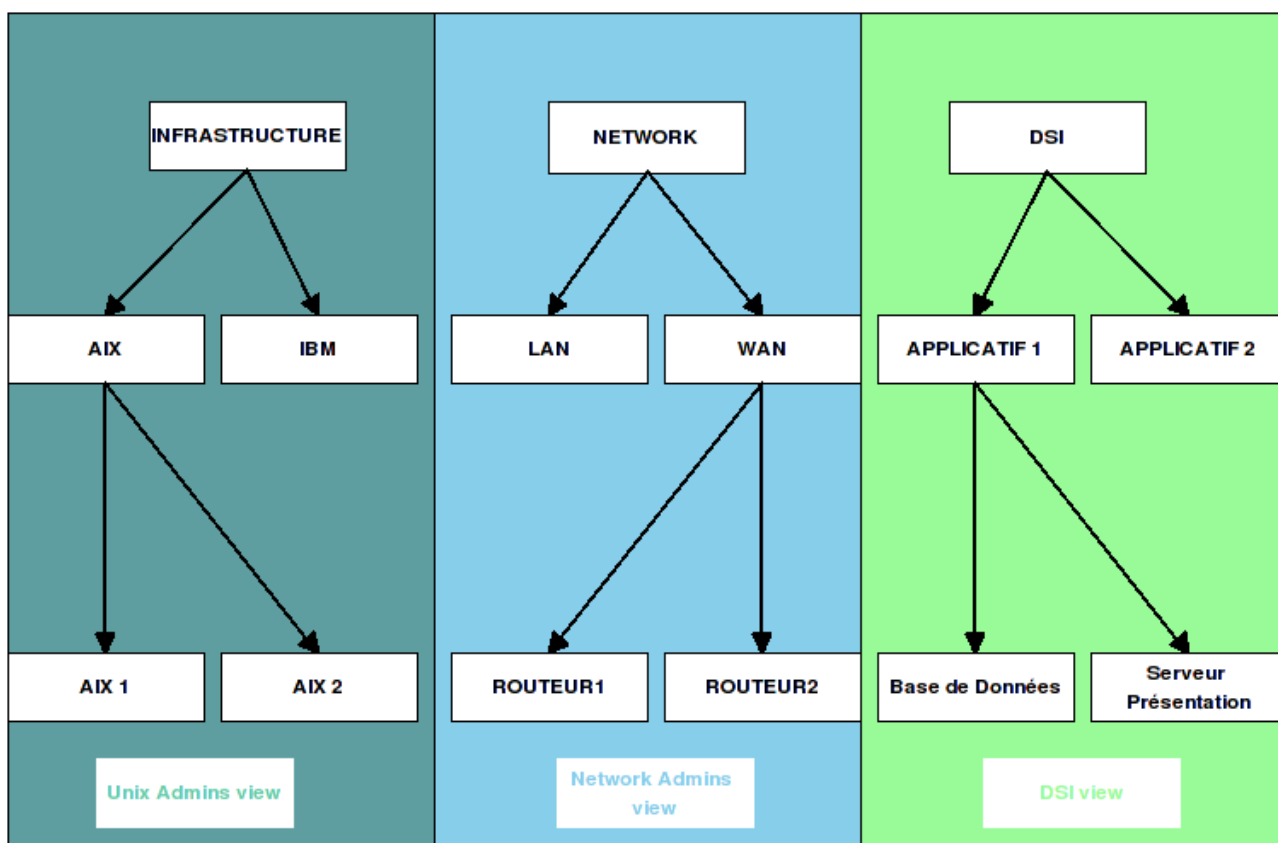


Figure 3 : Exemple de vues différenciées

1.4. Vue temps réel

La vue temps réel correspond à l'état du système d'information à l'instant de la visualisation. Nareto calcule l'état d'un noeud en fonction de l'état de ses noeuds inférieurs. L'état d'un noeud correspond à l'état le plus grave de tous ses sous noeuds. Par exemple, sur un applicatif n-tiers, l'état de cet applicatif sera l'état le plus grave de chacun des éléments le composant. Cette fonctionnalité facilite la navigation et la recherche de l'élément problématique.

En effet, lorsqu'un élément pose problème, automatiquement son état est remonté au niveau le plus haut. Il

suffit de parcourir l'arbre en profondeur (« drill-down ») en cliquant, à chaque niveau sur le noeud qui affiche l'état problématique pour arriver directement sur l'élément précis en cause (voir « Drill Down Niveau 1 » et « Drill Down Niveau 2 »). La navigation est simple et rapide.

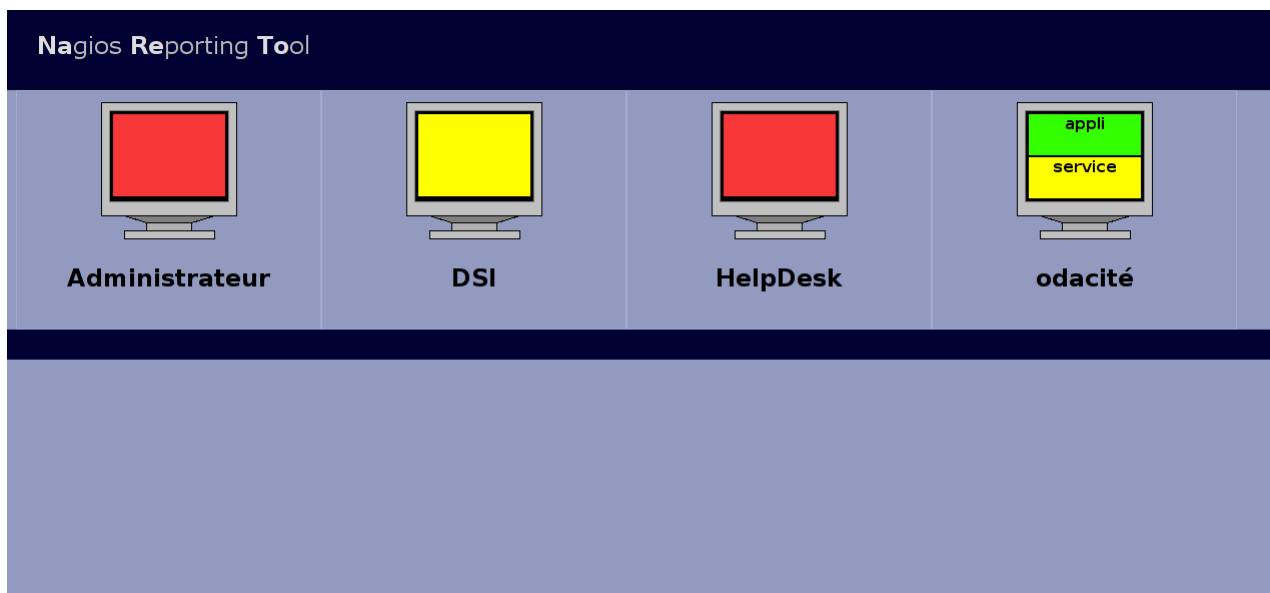


Figure 4 : Drill Down : niveau 1

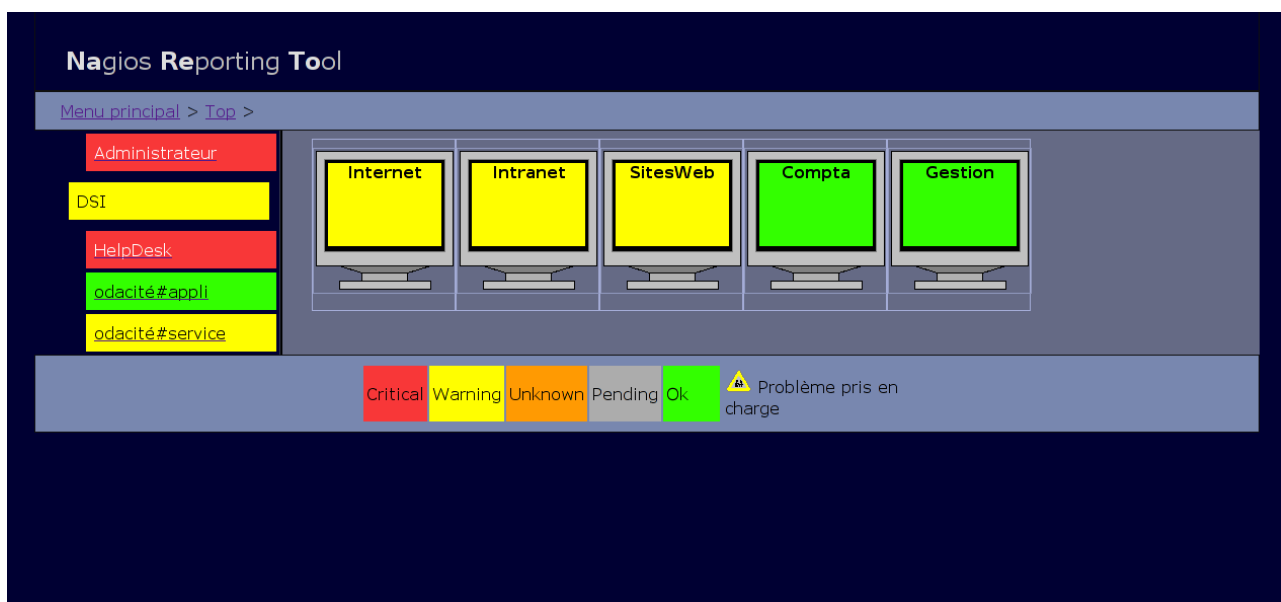


Figure 5 : Drill Down : Niveau 2

La vue temps réel affiche aussi la liste des indicateurs qui ont des données de performances. Il suffit de cliquer sur ce lien pour arriver directement sur le graphique de cet indicateur.

1.5.Reporting

Le reporting correspond au calcul de la disponibilité des différents noeuds. La disponibilité d'un noeud est calculé en pourcentage sur une période donnée. La période est libre : il suffit de sélectionner la date et l'heure de début puis la date et l'heure de fin pour obtenir les informations correspondantes. Là encore, on peut naviguer dans l'arbre en traversant les noeuds du niveau le plus haut vers le niveau le plus bas. Il est alors aisé de voir quel est le noeud ou l'indicateur qui a diminué le taux de disponibilité global. Les données affichées pour un noeud donné sont le poids de ce noeud dans le calcul de la disponibilité, le taux de disponibilité sur la période sélectionnée et un graphique affiche l'évolution du taux de disponibilité au cours du temps.

Le taux de disponibilité d'un noeud est calculé en fonction de l'état de ses sous noeuds. Un poids est affecté à chacun des sous noeuds. Plus le poids est important et plus l'état du noeud influe sur le calcul. Un noeud ayant un poids de 10 influe 2 fois plus qu'un noeud ayant un poids de 5 sur le calcul de la disponibilité du noeud de niveau supérieur.

Si le noeud est un indicateur sa valeur est calculé en fonction de l'état de cet indicateur dans Nagios. Par exemple, un indicateur dans l'état CRITICAL a pour taux de disponibilité 0%. Un indicateur dans l'état WARNING a pour taux de disponibilité 75%. Ces valeurs sont configurables.

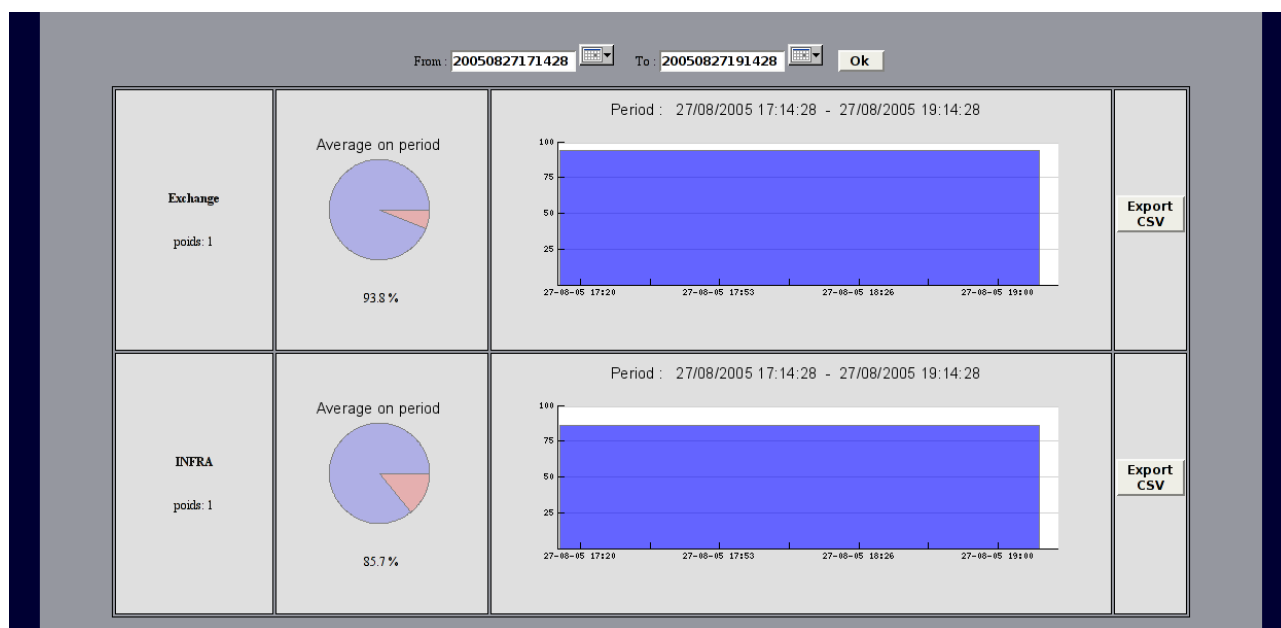


Figure 6 : Reporting

1.6.Suivi des alarmes

A chaque changement de l'état OK à un état d'erreur, Nagios génère une alarme. Dès que l'indicateur revient dans l'état OK, cette alarme est fermée. Dès qu'un utilisateur prend en compte cette alarme en faisant un ACK dans l'interface Nagios, l'état de cet indicateur est modifié pour afficher cette prise en compte. Ces informations sont insérées dans le fichier journal de Nagios.

Nareto lit régulièrement les fichiers journaux de Nagios, analyse les données et les insère en base de données. Ensuite, dans la vue de suivi des alarmes (voir « Suivi alarmes : affichage principal ») sont affichées les informations importantes sur ces alarmes. Les données sont agrégées dans les noeuds de plus haut niveau. Là encore, on navigue dans l'arbre et on peut suivre quel est le noeud ou l'indicateur qui génère le plus d'alarmes. De plus, la période de visualisation du suivi des alarmes est libre : il suffit de choisir la date de début et la date de fin.

Les informations affichées sont le nombre moyens d'alertes en fonction du temps, le temps moyen sur la période sélectionnée de prise en compte par un utilisateur et le temps moyen de retour à l'état normal de l'indicateur. Un export des informations au format CSV (Comma Separated Values) pour chacun des noeuds est disponible (voir « Suivi des alarmes : export CSV »).

Il est aussi possible d'afficher les alarmes de la dernière semaine avec le détail complet de cette alarme : l'indicateur qui a généré cette alarme, la date, la description de cette alarme, la date de prise en compte, l'utilisateur qui a pris en compte cette alarme avec le texte de prise en compte et la date de correction (voir « Suivi des alarmes : alarmes de la semaine »).

[Menu principal](#) > [Racine](#) >

Début 2005-06-01

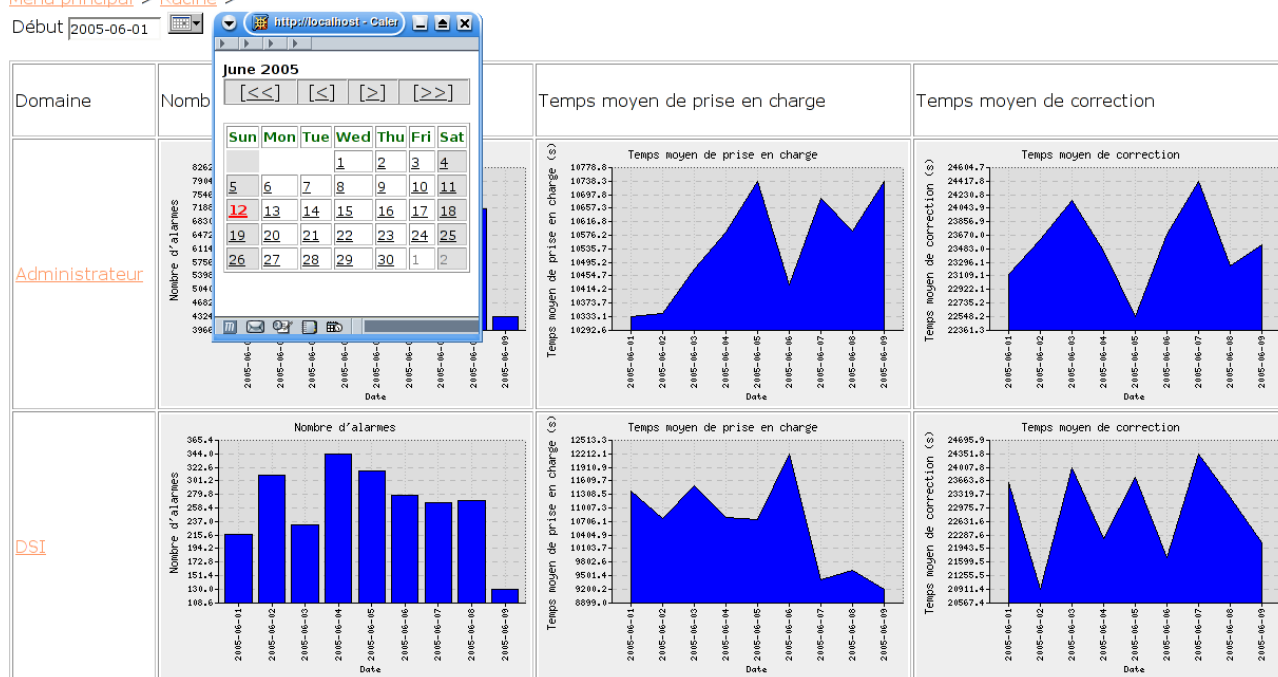


Figure 7 : Suivi des alarmes : affichage principal avec choix de période

Menu principal > Racine > Administrateur

Début 2005-06-12 Fin 2005-06-18 Valider

Host	Service	Corrigé?	Date de l'alarme	Texte	Ackeur	Date du ack	Date de correction	Commentaire
localhost_1_2	smtp	Yes	2005-06-12 11:52:34	Connection refused			2005-06-12 10:57:22	
localhost_1_1	smtp	Yes	2005-06-12 11:52:35	Connection refused			2005-06-12 10:57:22	
localhost_1	smtp	Yes	2005-06-12 11:52:35	Connection refused			2005-06-12 10:57:22	
localhost	smtp	Yes	2005-06-12 11:52:35	Connection refused			2005-06-12 10:57:22	
localhost_1_5	CPU	Yes	2005-06-12 11:52:36	WARNING - load average: 2.12, 0.94, 0.55			2005-06-12 11:31:32	
localhost_1_4	CPU	No	2005-06-12 11:27:32	WARNING - load average: 2.12, 0.94, 0.55				
localhost_2	CPU	Yes	2005-06-12 11:52:36	WARNING - load average: 2.12, 0.94, 0.55			2005-06-12 11:31:32	
localhost_1_3	CPU	No	2005-06-12 11:27:32	WARNING - load average: 2.12, 0.94, 0.55				
localhost	CPU	Yes	2005-06-12	WARNING - load average: 2.27, 1.08,			2005-06-12	

Figure 8 : suivi des alarmes : alarmes de la semaine

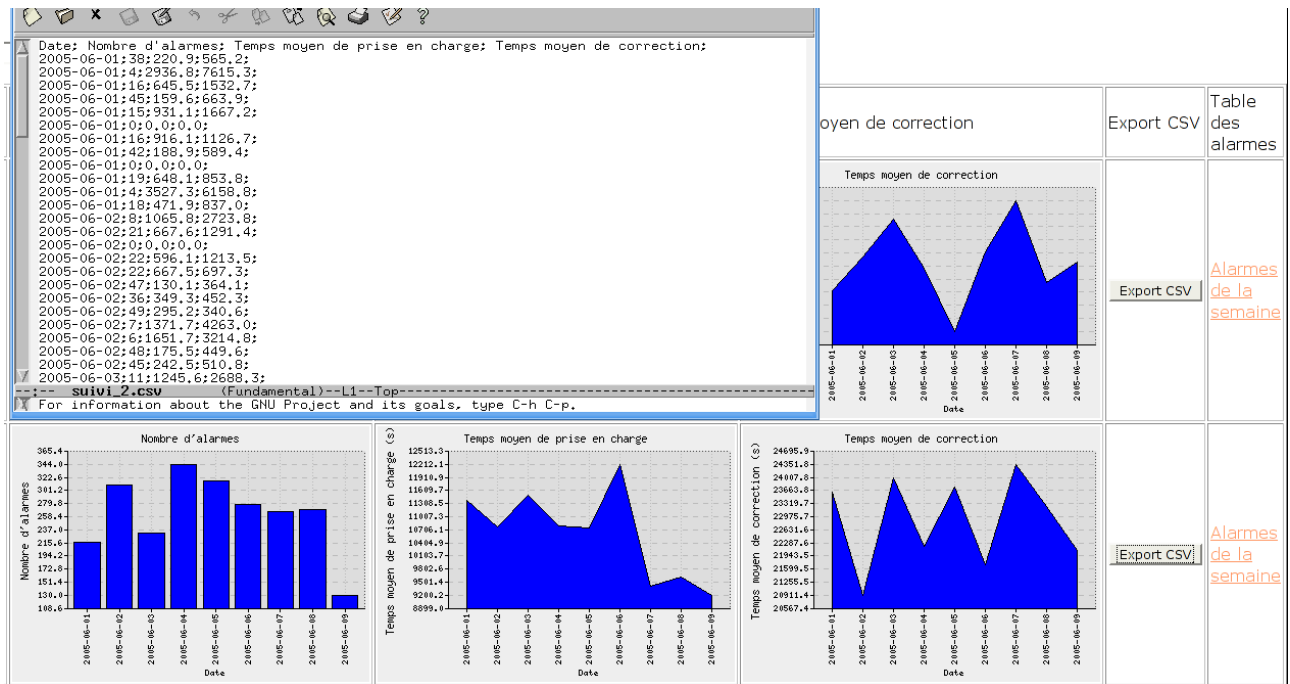


Figure 9 : Suivi des alarmes : export CVS