

Introduction

Opmanager est un outil de supervision des équipements réseau. Il supporte SNMP, WMI et des scripts ssh ou Telnet pour récupérer des informations sur les machines. Toutefois les machines doivent posséder un agent SNMP pour être gérée par **Opmanager**. Cet outil est gratuit pour une utilisation jusqu'à 20 machines, la version complète intègre des modules en plus qui permettent notamment de gérer l'Active directory des contrôleurs de domain, les serveurs Exchange, MS SQL serveur et un module de notification par SMS.

C'est une application Windows téléchargeable à l'adresse suivante :

<http://manageengine.adventnet.com/products/opmanager/download.html?free>

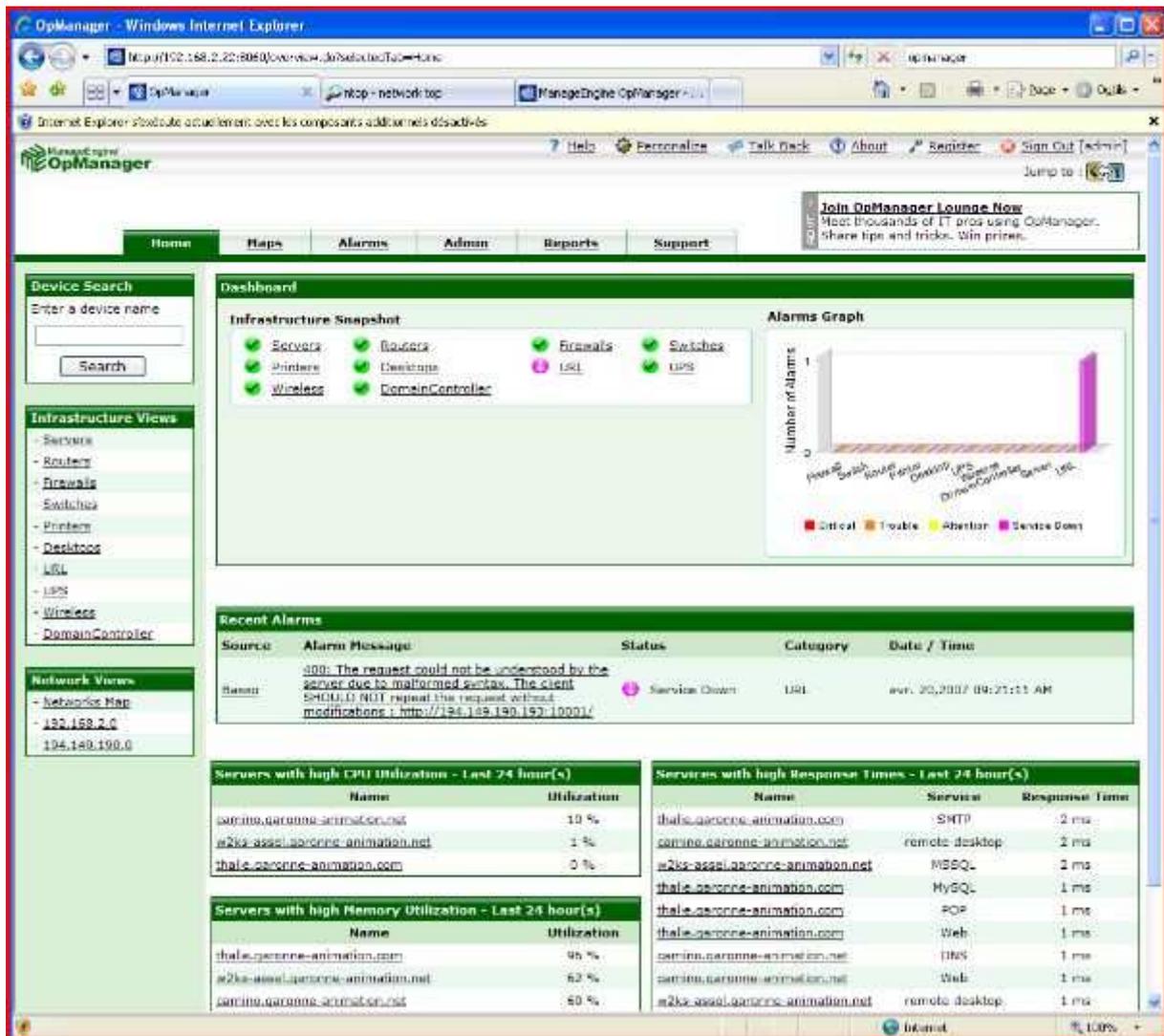
Cette application installe un serveur Web pour l'administration et un serveur SQL ou peut utiliser un serveur SQL existant.

Présentation du produit Opmanager

Voilà vous avez fini l'installation vous allez vous connectez sur l'interface d'admin pour la première fois (admin/admin) par défaut.

La première page affichée présente un état des ressources réseau :

- ❖ alarmes récentes
- ❖ serveurs avec le plus haut taux d'utilisation de la CPU
- ❖ serveurs utilisant le plus de mémoire
- ❖ les services qui répondent le plus lentement



L'interface possède plusieurs onglets qui vont vous permettre d'effectuer toutes les actions possibles :

- ❖ maps affiche les machines disponibles dans le réseau en cours
- ❖ alarms liste les alarmes en cours
- ❖ admin affiche l'interface d'administration à partir de laquelle on peut modifier tous les paramètres de l'application
- ❖ reports permet de générer des rapports prédéfinis ou personnalisés.
- ❖ Support permet de consulter et d'envoyer des messages au support en cas de problèmes.

En fonction de l'onglet sur lequel on se positionne le menu à gauche change et affiche les actions correspondantes.

Prise en compte des équipements

Ajouter une machine

Pour ajouter une machine il suffit d'aller sur l'onglet admin et de cliquer sur le bouton « Add device ».

Admin > Add Device



Add Device	
Device name / IP Address	<input type="text"/>
Netmask	<input type="text" value="255.255.255.0"/>
SNMP Port	<input type="text" value="161"/>
Community String	<input type="text" value="•••••••"/>
<input type="button" value="Add Device"/>	

Il est impératif qu'un agent snmp soit actif sur le périphérique que vous souhaitez ajouter. Entrez le nom ou l'adresse IP du périphérique changez les autres paramètres si cela est nécessaire et cliquez sur add device.

Vous pouvez maintenant retrouver la machine en cliquant sur l'onglet « HOME » puis sur le sous réseau auquel elle appartient.

Configuration des notifications

A partir de l'onglet Admin cliquez sur « notification profiles » dans la rubrique « global settings ». Ces profiles pourront être associés à différents périphériques.

Si vous ne l'avez pas encore fait Opmanager va vous demander de configurer un serveur de messagerie afin qu'il puisse envoyer des notifications par email.



Mail server settings	
Server name	<input type="text" value="192.168.2.254"/>
Port	<input type="text" value="25"/> (e.g., 25)
	<input type="checkbox"/> Requires Authentication
User name	<input type="text"/>
Password	<input type="text"/>
From Email ID (optional)	<input type="text" value="Notification@opmanager.c"/> (The default from mail id for all notifications)
To Email ID	<input type="text" value="marc.tecles@garonne-anir"/> <input type="button" value="Send a test message"/> (The default mail id to which all the notifications will be sent.)
	<input type="checkbox"/> Add a secondary mail server (optional)
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

- ❖ entrez le nom ou l'adresse IP du serveur de messagerie
- ❖ entrez si nécessaire les informations d'authentification
- ❖ Entrez dans « To Email ID » l'adresse qui recevra les alertes. Il est recommandé d'utiliser le bouton « send a Test Message » pour vérifier que la configuration fonctionne est que vous recevez bien les messages d'alerte.

Notifications

Nous allons maintenant voir comment configurer les différentes options de notifications.



Nous avons les possibilités suivantes :

- ❖ émission d'un email
- ❖ envois d'un sms par modem
- ❖ envois d'un sms par email
- ❖ exécution de commande
- ❖ loggé l'information dans une appli externe de gestion d'incident (payant)

Nous allons nous concentrer sur la configuration des notifications par email les autres méthodes présentant peu d'intérêt ou étant payantes.

Dans le menu « Add New » cliquez sur « Email Alert »

Vous pouvez choisir l'adresse du destinataire qui recevra les alertes pour les périphériques associés à ce profil de notification.

Vous pouvez aussi modifier le contenu du message à l'aide des listes de variables disponibles. Cliquez sur **save** une fois terminé.

Association d'un profil au device

Maintenant il ne vous reste plus qu'à associer ce profil avec votre machine. Pour cela toujours dans la fenêtre « notification profiles » cliquez sur « **associate to devices** » dans le menu actions à droite.

On sélectionne le profile créé précédemment dans la liste puis on clique « next »

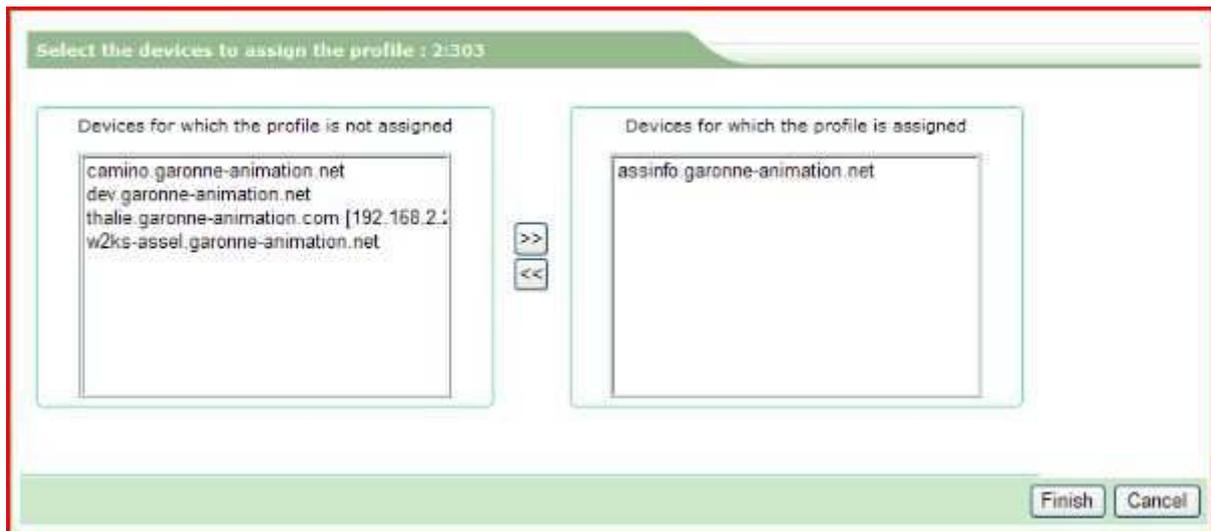


On va maintenant choisir dans quels cas un message d'alerte doit être émis.

- ❖ Si le périphérique n'a pas répondu à 1 test
- ❖ Quand l'interface ou le port du switch est arrêté
- ❖ Quand n'importe lequel des services sélectionnés dans la liste est arrêté
- ❖ Quand n'importe lequel des services Windows sélectionnés est arrêté
- ❖ Si une interruption SNMP est reçue
- ❖ Quand n'importe lequel des seuils a été dépassé
- ❖ Quand n'importe laquelle des règles du journal d'événement a généré une alarme.
- ❖ Quand l'alarme est annulée



On peut lier le profile a une des catégories de périphérique prédéfinies (Router, server ...) ou sélectionner manuellement les périphériques.



A gauche la liste de tous les périphériques déclarés dans notre système, à droite les périphériques attachés à ce profile de notification.

Cliquez sur Finish .

Sélection des ressources à surveiller

Maintenant que votre machine a été ajoutée vous pouvez choisir les ressources à surveiller. Par défaut lors de l'ajout d'une machine le logiciel scanne la machine pour détecter la présence de certains services bien connus (http, ftp, sql, smtp, pop ...). Voici une liste des ressources présent en charge par défaut.

- ❖ services détectés lors de l'ajout de la machine
- ❖ interfaces réseau détectées
- ❖ CPU
- ❖ Mémoire
- ❖ Utilisation des disques

Si la machine est un serveur et possède plusieurs disque l'utilisation disques n'est pas vraiment intéressante car elle affiche un pourcentage d'utilisation des disques de la machines. Cela ne nous permet pas de voir si un disque en particulier n'a plus d'espace libre.

Voici les différents types d'informations que nous allons pouvoir surveiller :

- ❖ service monitor : les services réseau actifs sur la machine exemple http 80, smtp 25 etc...
- ❖ Windows service monitors : les services Windows exemple MSSQL\$XX pour le serveur SQL
- ❖ Url monitors :
- ❖ Ressource monitor : cpu, mémoire, disque, espace libre sur les disques, liste des processus...

- ❖ Traffic monitors : Infos sur le trafic réseau
- ❖ Application monitors : permettent de surveiller finement des applications MSSQL, Exchange etc il faut la version complète pour cela.
- ❖ Vendor specific monitors : des compteurs spécifiques à un vendeur exemple Cisco, Dell, compaq etc...
- ❖ Pour ajouter ou modifier un compteur il faut à partir de la fiche du périphérique:
- ❖ allez dans la rubrique correspondante exemple « ressource monitors » et cliquez sur « ADD Monitor »

The screenshot shows the 'Resource Monitors' window with a status bar indicating 'Total monitors 5, None in error' and an '+ Add Monitor' button. Below is a table listing the configured monitors.

<input type="checkbox"/>	Monitors	Monitor Type	Polling Interval (mins)	Threshold	Edit
<input type="checkbox"/>	CPU Utilization	SNMP	3	Not Enabled	
<input type="checkbox"/>	Disk Utilization	SNMP	60	Not Enabled	
<input type="checkbox"/>	Free Disk Space in MB - C:\ Label: Serial Number 4c0158f4	SNMP	5	Normal	
<input type="checkbox"/>	Free Disk Space in MB - D:\ Label: Serial Number 40a8c372	SNMP	5	Normal	
<input type="checkbox"/>	Memory Utilization	SNMP	15	Not Enabled	

At the bottom left of the table area is a 'Remove' button.

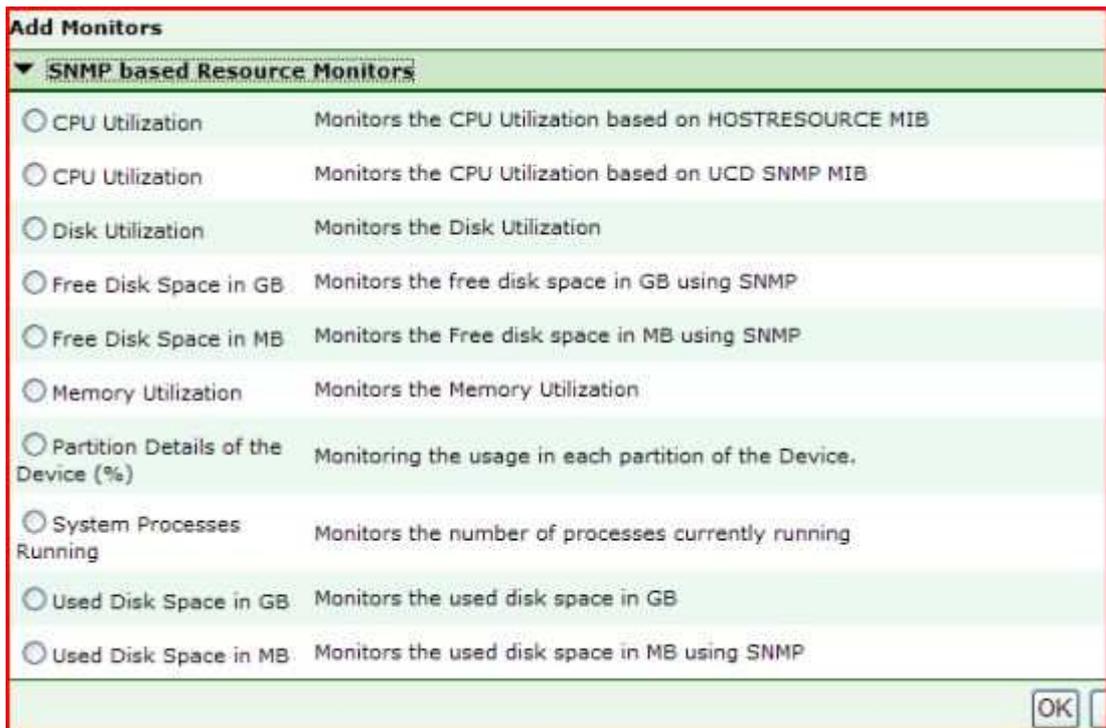
Méthode de collecte des informations

Dans la liste sélectionnez la méthode à utiliser pour récupérer les informations exemple SNMP

The screenshot shows the 'Add Monitors' dialog box with a list of monitor types, each preceded by a right-pointing arrow.

Add Monitors
▶ SNMP based Resource Monitors
▶ WMI based Monitors
▶ Telnet/SSH based monitors for Linux
▶ Telnet/SSH based monitors for Solaris
▶ Cisco Monitors
▶ 3COM
▶ Printer
▶ Fortigate
▶ Netscreen
▶ HP ProCurve
▶ Telnet based graphs for IBM AIX
▶ Telnet based graphs for HP-UX

- ❖ enfin sélectionnez le compteur et cliquez sur OK



Certains compteurs nécessitant des paramètres afficheront une page en plus avec ces paramètres. Exemple pour espace disque libre il faudra choisir les disques à surveiller.

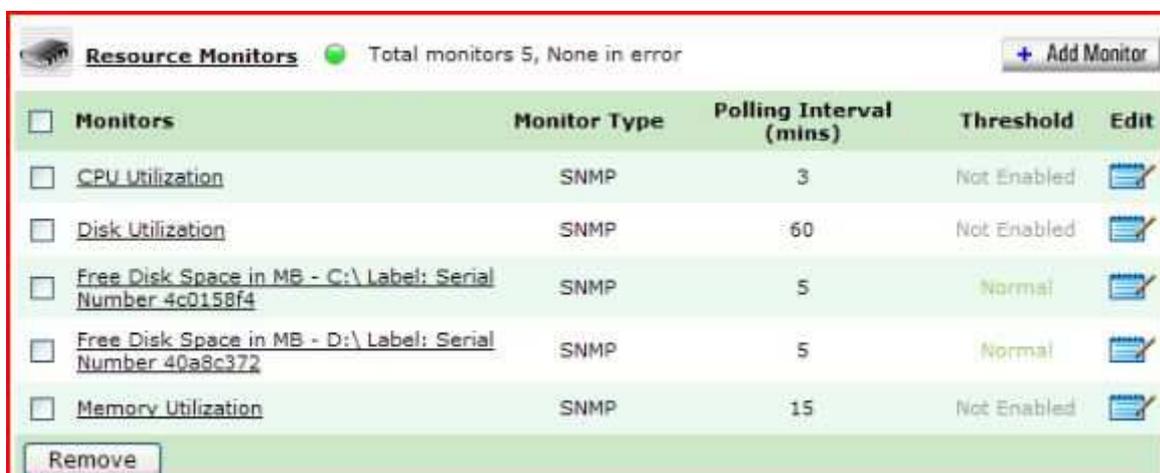
Une fois le compteur ajouté il apparait automatiquement dans la liste correspondante. Vous pouvez ensuite avec le petit bouton **edit** changer les options, fréquence d'interrogation du compteur, et mise en place d'un seuil d'alerte.

Mise en place de seuils d'alertes

Bien entendu il faut au préalable avoir ajouter un compteur sur la valeur avant de pouvoir mettre en place un seuil sur cette dernière.

❖ A partir de la fiche du périphérique :

Allez dans la rubrique correspondante exemple « **ressource monitors** » et cliquez sur « edit » sur la ligne correspondante à votre compteur.



- ❖ cochez la case enable threshold

Edit Monitor

Monitor Properties

Monitor Name : **MemoryUtilization**

Display Name : **Memory Utilization**

Polling Interval (mins) :

Units : **Percentage**

Threshold Settings (optional)

Enable Threshold

Threshold allow you to set safe limit for the data collected for graphs. OpManager can be configured to send notifications if the limit is violated.

Threshold Limit : eg. 70 (or) 95 etc

Threshold Check : Monitored value is threshold limit.

Alarm Message :
(This message will be sent as the Alarm)

Severity of the Alarm :

Generate Alarm, only if threshold is violated consecutive times.

Clear Alarm Generation

Threshold Check : Monitored value is threshold limit.

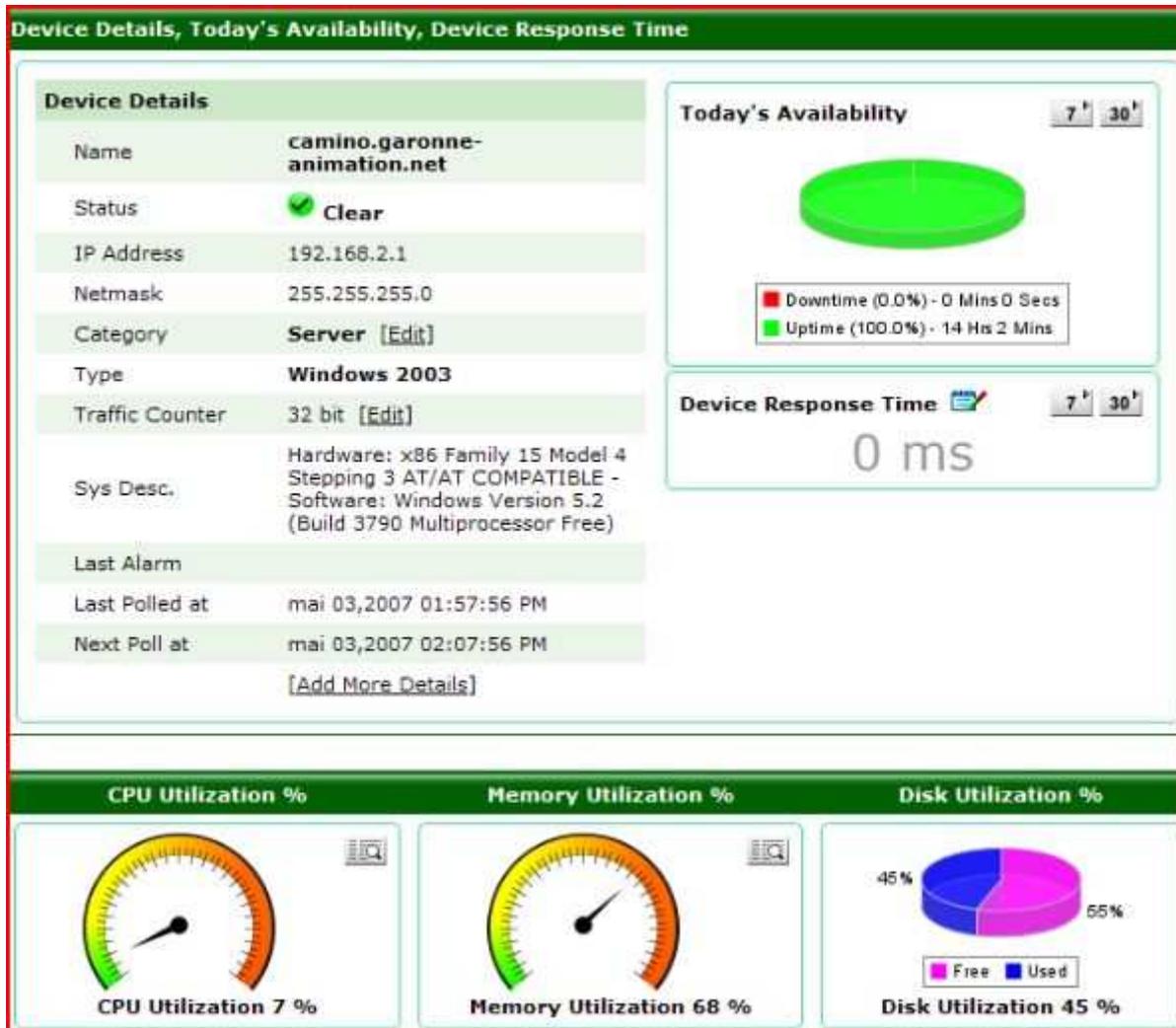
Rearm Value :

- ❖ saisissez la valeur du seuil dans « **threshold limit** » qui peut être une limite haute ou basse il suffit de sélectionner « **greater than** » ou « less than » dans threshold check.
- ❖ Saisissez un message dans alarm Message il sera envoyé par email.
- ❖ Indiquez le niveau de sévérité de l’alarme
- ❖ Indiquez le nombre de fois que le seuil doit être dépassé avant qu’une alarme ne soit générée.
- ❖ Rearm Value indiquez la valeur du compteur pour laquelle l’alarme doit être désactivée.
- ❖ Maintenant vous recevrez des emails si le seuil mis en place est dépassé.

Visualisation de l'état des ressources

Il existe plusieurs façons de visualiser l'état d'un périphérique.

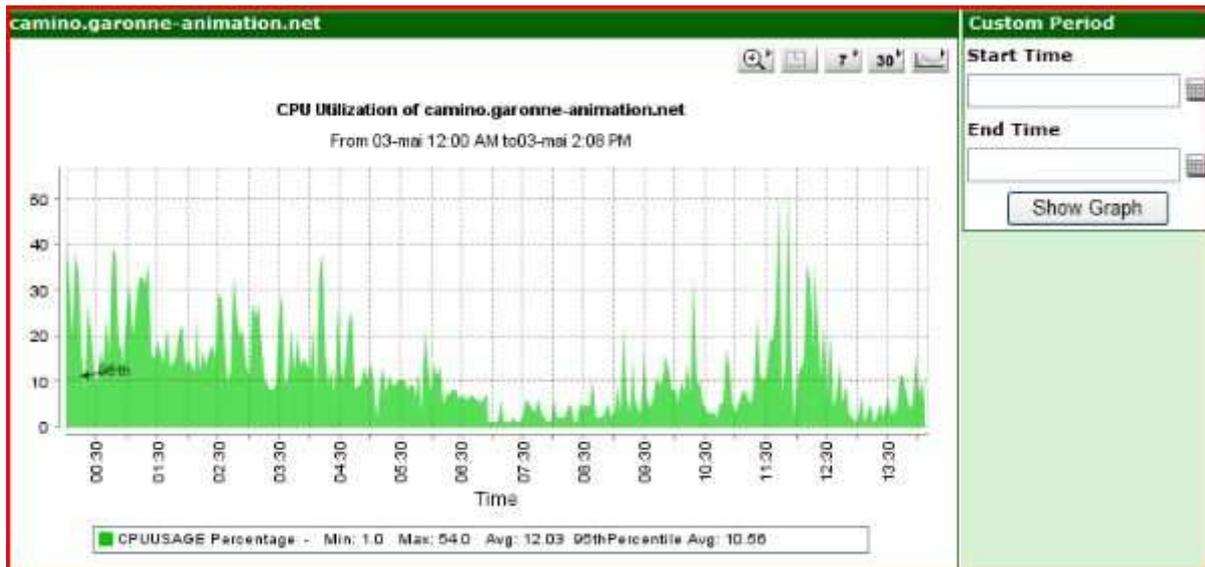
- ❖ résumé des informations sur la fiche d'un périphérique



On a un aperçus de l'utilisation CPU, de la mémoire et des disques ainsi que la disponibilité de la machine sur la journée en cours.

- ❖ plus détaillé en cliquant sur les dessins.

Exemple utilisation CPU



On a la possibilité ici de zoomer, de voir les 7 derniers jours, les 30 derniers d'un clique ou bien de changer la période que l'on souhaite afficher avec les champs start et end time.

Ces opérations sont possibles avec tous les compteurs mise en place.

Planification et consultation des rapports

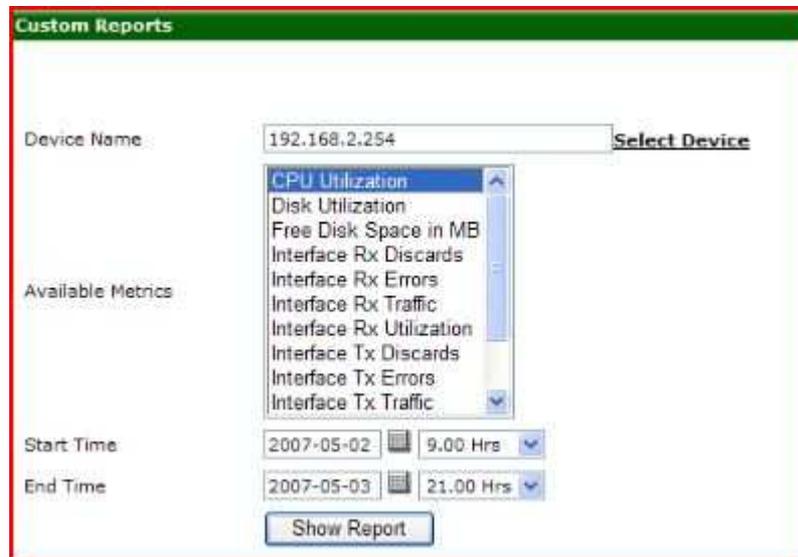
Il existe beaucoup de rapports prédéfinis que vous pouvez utiliser

Servers	
Report Name	Description
Top 10 Reports	
Servers by CPU Utilization	Identify busy servers with high CPU Utilization
Servers by Memory Utilization	Identify overloaded servers with high Memory Utilization
Servers by Disk Utilization	Identify overloaded servers with high Disk Utilization
Servers by Rx Traffic	Identify servers with heavy incoming traffic
Servers by Tx Traffic	Identify servers with heavy outgoing traffic
Servers by Rx Utilization	Identify servers with heavy incoming traffic utilization
Servers by Tx Utilization	Identify servers with heavy outgoing traffic utilization
Volumes with Least Free Space	Identify disk partitions with least free space
Volumes with Most Free Space	Identify disk partitions with most free space
Detailed Reports	
All Servers Disk Usage Report	Get partition wise disk usage report for all servers
All Servers Availability Report	Get availability report for all servers

Ceci n'est qu'une partie des rapports prédéfinis.

De plus vous pouvez créer des rapports personnalisés

Dans l'onglet rapport cliquez sur « **Run a custom report** »



Custom Reports

Device Name: 192.168.2.254 [Select Device](#)

Available Metrics:

- CPU Utilization
- Disk Utilization
- Free Disk Space in MB
- Interface Rx Discards
- Interface Rx Errors
- Interface Rx Traffic
- Interface Rx Utilization
- Interface Tx Discards
- Interface Tx Errors
- Interface Tx Traffic

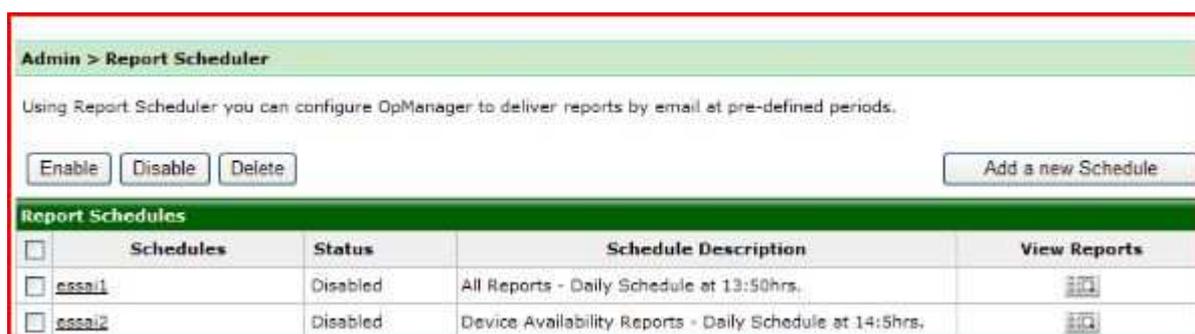
Start Time: 2007-05-02 9:00 Hrs

End Time: 2007-05-03 21:00 Hrs

[Show Report](#)

- ❖ Choisir un périphérique avec select device
- ❖ Choisir les compteurs à afficher dans le rapport
- ❖ Choisir la période
- ❖ Cliquez sur show report

Vous avez la possibilité d'exporter le rapport au format pdf ou de l'imprimer. Enfin vous avez la possibilité de planifier l'exécution d'un rapport. Pour cela dans l'onglet « admin » cliquez sur « schedule reports » dans la rubrique tools.



Admin > Report Scheduler

Using Report Scheduler you can configure OpManager to deliver reports by email at pre-defined periods.

[Enable](#) [Disable](#) [Delete](#) [Add a new Schedule](#)

<input type="checkbox"/>	Schedules	Status	Schedule Description	View Reports
<input type="checkbox"/>	rssa1	Disabled	All Reports - Daily Schedule at 13:50hrs.	View
<input type="checkbox"/>	rssa2	Disabled	Device Availability Reports - Daily Schedule at 14:5hrs.	View

cliquez sur « **Add a new Schedule** »

Schedule name:

Choose Report Type

Device specific Availability reports

Top N Reports / All Devices reports

Saisissez un nom et le type de rapport

Generate Availability Reports for the Selected Types

Generate Availability Report to all devices in this Category:

Manually Group Devices to generate Availability Report

Select a period for Availability Report:

Sélectionnez la période et les périphériques sur lesquels va porter notre rapport

Select devices to generate availability report.

Devices Available

- dev.garonne-animation.net
- thalie.garonne-animation.com [192.168.2.]
- w2ks-assel.garonne-animation.net

Devices Selected

- assinfo.garonne-animation.net
- camino.garonne-animation.net

>>

Sélection manuelle des périphériques

Time

Daily
 Weekly
 Monthly

Time : 9 hrs 00 mins

Report Delivery

Send the report as attachment to**

Publish the reports and send the url alone to

Back Next Cancel

Sélectionnez la périodicité avec laquelle le rapport sera exécuté. Choisissez la méthode d'envoi du rapport par email, pièce jointe ou liens.

Schedule name : Monrapport

Report Type : Device Availability Reports

Report output format : PDF (.pdf, Portable Document Format)

Time & Delivery
 Reports will be Generated Daily at 9:00 hrs.

Publish Details
 The Published Report URL will be sent to marc.tecles@garonne-animation.com.

Selected Devices

Back Submit Cancel

Un petit récapitulatif pour finir. Puis après un clique sur « Submit » votre rapport apparaîtra dans la liste avec un status enable qui indique qu'il est actif.