

# Analyse des systèmes

Cours Windows 2008-2009

Franck Rupin - Laurent Gydé

# 1 Les concepts d'analyse

L'analyse des performances d'un système permet d'obtenir des informations sur ce système qui serviront de référence pour une utilisation optimale.

Les données recueillies permettront d'établir des seuils de dégradation des performances système.

# 1 Les concepts d'analyse

Ces valeurs de référence fourniront une aide pour déterminer la cause de pannes qui surviendront.

De plus elles permettront aussi à l'ingénieur système de planifier les évolutions à apporter au système en fonction de la croissance de sa charge.

# 1 Les concepts d'analyse

L'analyse des performances mesure le taux d'utilisation des ressources du système et la manière dont elles sont exploitées par les différents processus.

On peut distinguer 4 groupes majeurs de ressources :

- La mémoire

- Le(s) processeur(s)

- Le(s) disque(s)

- Les éléments réseau

# 1 Les concepts d'analyse

**La notion de débit :**

Il s'agit de la mesure du travail effectué en une unité de temps.

Le débit croît en fonction de la croissance de la charge jusqu'à un seuil.

Une fois atteint ce seuil, le débit chute. Une file d'attente peut en résulter.

# 1 Les concepts d'analyse

Le débit général du système est déterminé par l'élément le plus faible.

Cet élément le plus faible est défini comme un goulet d'étranglement.

L'analyse des performances doit aider à la détection des goullets d'étranglement.

# 1 Les concepts d'analyse

## File d'attente :

Les conditions de formation d'une file d'attente peuvent-être diverses:

Les requêtes pour une ressources arrivent plus vite que le débit de la ressource

Les requêtes sont produites à intervalles irréguliers : lots de requêtes importants, puis inactivité.

# 1 Les concepts d'analyse

Si une file d'attente devient trop longue, le travail risque de ne plus être géré.



# 1 Les concepts d'analyse

**Temps de réponse :**

Temps nécessaire pour effectuer un travail totalement.

Le temps de réponse croît en fonction de la charge :

Soit  $W$  le travail,  $F$  la longueur de la file,  $D$  le débit de la ressource:

$$W = F/D$$

# 2 Les outils d'analyse de Windows

1 Concepts d'analyse

2 les outils d'analyse de Windows

3 Les goulets d'étranglement

## 2 Les outils d'analyse de Windows

**Les données collectées :**

Les données relatives aux différents compteurs des objets analysées, sont collectées à partir du registre.

Ils s'agit d'informations relatives à la mémoire, au processeur, aux disques, au réseau.

WMI (windows management instrumentation), permet aussi de collecter des données au lieu d'utiliser le registre:

Par exemple la commande ***perfmon /wmi*** emploiera cette méthode alors que ***perfmon*** utilisera le registre.

## 2 Les outils d'analyse de Windows

Les objets de performance représentent des ressources matérielles ou système.

Exemples :

Mémoire

NBT

ICMP

IP

Processeur

Processus

## 2 Les outils d'analyse de Windows

Chaque objet se voit attribuer des compteurs de performance, qui lui sont propres.

Ces compteurs sont relatifs à la nature de l'objet :

- Taux de transfert pour un disque

- Temps processeur pour un processus

# 2 Les outils d'analyse de Windows

## Les outils de Windows :

### Le gestionnaire de tâches `taskmgr.exe`

Pour lancer le gestionnaire de tâches il suffit d'exécuter CTRL+ALT+SUPPR puis cliquer sur l'onglet gestionnaire de tâches.

Vous pouvez aussi taper ***taskmgr*** dans le menu démarrer/exécuter ou à partir d'une invite de commande.

## 2 Les outils d'analyse de Windows

Le gestionnaire de tâches permet d'effectuer une analyse du système, mais c'est un outil limité.

Il n'offre pas, par exemple de fonctionnalité de journalisation ni d'alerte.

Il permet les actions suivantes:

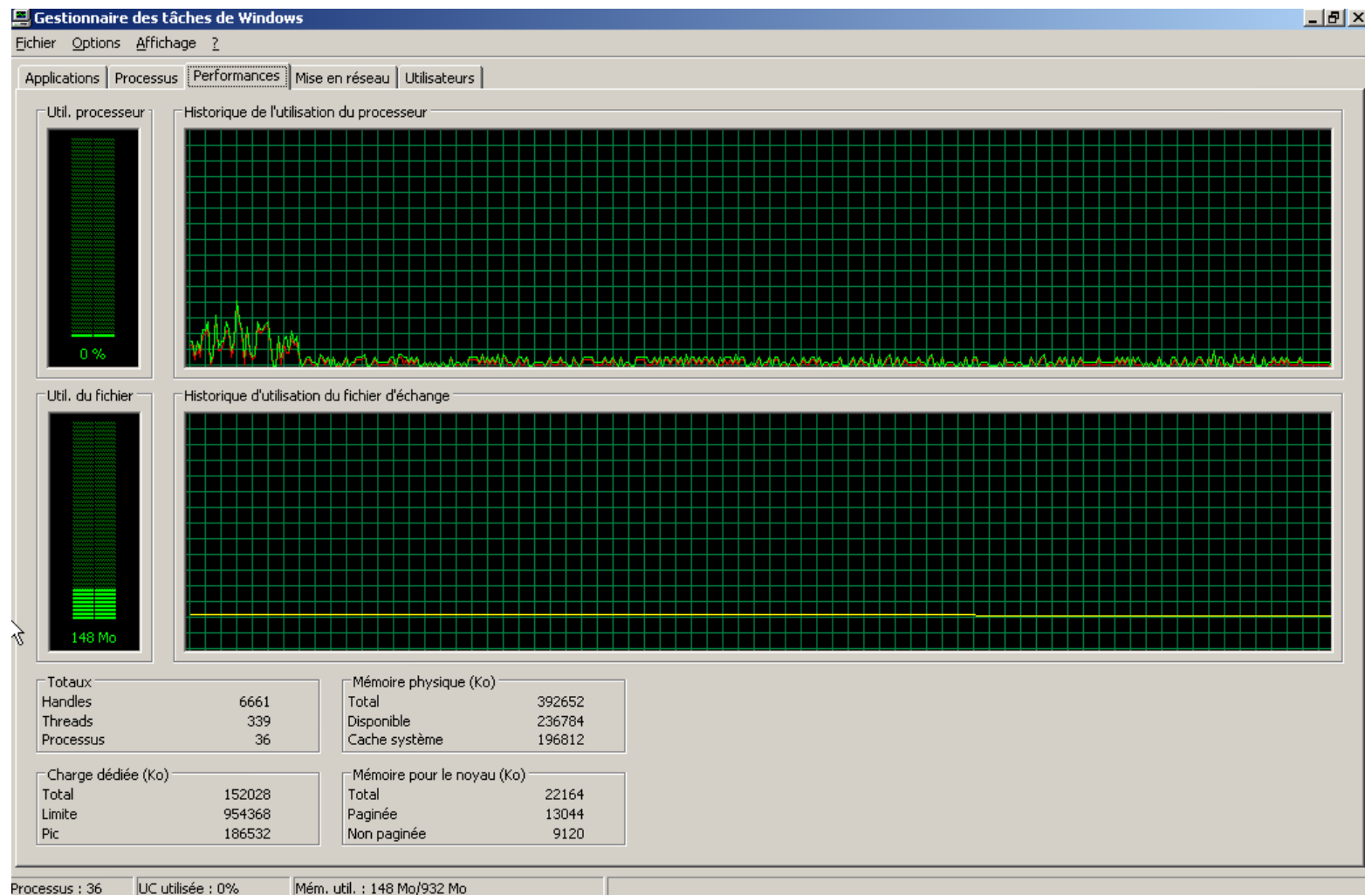
- Stopper des processus

- Changer la priorité d'un processus

- D'observer l'activité du (des) processeur(s), des disques, de la mémoire, du réseau, et les connexions utilisateurs.

# 2 Les outils d'analyse de Windows

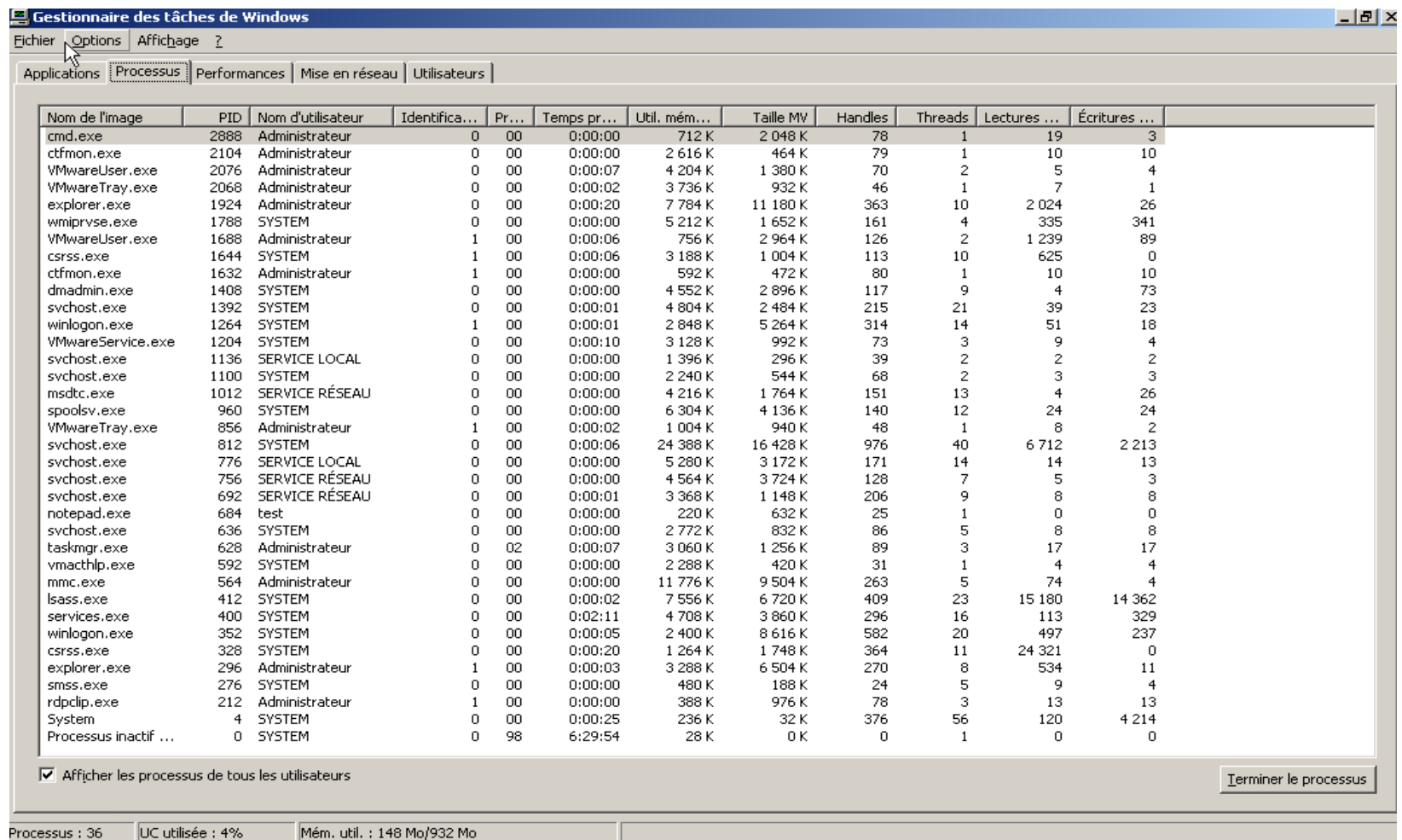
## Onglet performances





# 2 Les outils d'analyse de Windows

## Onglet processus



Gestionnaire des tâches de Windows

Fichier Options Affichage ?

Applications Processus Performances Mise en réseau Utilisateurs

Nom de l'image	PID	Nom d'utilisateur	Identifica...	Pr...	Temps pr...	Util. mém...	Taille MV	Handles	Threads	Lectures ...	Écritures ...
cmd.exe	2888	Administrateur	0	00	0:00:00	712 K	2 048 K	78	1	19	3
ctfmon.exe	2104	Administrateur	0	00	0:00:00	2 616 K	464 K	79	1	10	10
VMwareUser.exe	2076	Administrateur	0	00	0:00:07	4 204 K	1 380 K	70	2	5	4
VMwareTray.exe	2068	Administrateur	0	00	0:00:02	3 736 K	932 K	46	1	7	1
explorer.exe	1924	Administrateur	0	00	0:00:20	7 784 K	11 180 K	363	10	2 024	26
wmiprvse.exe	1788	SYSTEM	0	00	0:00:00	5 212 K	1 652 K	161	4	335	341
VMwareUser.exe	1688	Administrateur	1	00	0:00:06	756 K	2 964 K	126	2	1 239	89
csrss.exe	1644	SYSTEM	1	00	0:00:06	3 188 K	1 004 K	113	10	625	0
ctfmon.exe	1632	Administrateur	1	00	0:00:00	592 K	472 K	80	1	10	10
dmadmin.exe	1408	SYSTEM	0	00	0:00:00	4 552 K	2 896 K	117	9	4	73
svchost.exe	1392	SYSTEM	0	00	0:00:01	4 804 K	2 484 K	215	21	39	23
winlogon.exe	1264	SYSTEM	1	00	0:00:01	2 848 K	5 264 K	314	14	51	18
VMwareService.exe	1204	SYSTEM	0	00	0:00:10	3 128 K	992 K	73	3	9	4
svchost.exe	1136	SERVICE LOCAL	0	00	0:00:00	1 396 K	296 K	39	2	2	2
svchost.exe	1100	SYSTEM	0	00	0:00:00	2 240 K	544 K	68	2	3	3
msdtc.exe	1012	SERVICE RÉSEAU	0	00	0:00:00	4 216 K	1 764 K	151	13	4	26
spoolsv.exe	960	SYSTEM	0	00	0:00:00	6 304 K	4 136 K	140	12	24	24
VMwareTray.exe	856	Administrateur	1	00	0:00:02	1 004 K	940 K	48	1	8	2
svchost.exe	812	SYSTEM	0	00	0:00:06	24 388 K	16 428 K	976	40	6 712	2 213
svchost.exe	776	SERVICE LOCAL	0	00	0:00:00	5 280 K	3 172 K	171	14	14	13
svchost.exe	756	SERVICE RÉSEAU	0	00	0:00:00	4 564 K	3 724 K	128	7	5	3
svchost.exe	692	SERVICE RÉSEAU	0	00	0:00:01	3 368 K	1 148 K	206	9	8	8
notepad.exe	684	test	0	00	0:00:00	220 K	632 K	25	1	0	0
svchost.exe	636	SYSTEM	0	00	0:00:00	2 772 K	832 K	86	5	8	8
taskmgr.exe	628	Administrateur	0	02	0:00:07	3 060 K	1 256 K	89	3	17	17
vmacthlp.exe	592	SYSTEM	0	00	0:00:00	2 288 K	420 K	31	1	4	4
mmc.exe	564	Administrateur	0	00	0:00:00	11 776 K	9 504 K	263	5	74	4
lsass.exe	412	SYSTEM	0	00	0:00:02	7 556 K	6 720 K	409	23	15 180	14 362
services.exe	400	SYSTEM	0	00	0:02:11	4 708 K	3 860 K	296	16	113	329
winlogon.exe	352	SYSTEM	0	00	0:00:05	2 400 K	8 616 K	582	20	497	237
csrss.exe	328	SYSTEM	0	00	0:00:20	1 264 K	1 748 K	364	11	24 321	0
explorer.exe	296	Administrateur	1	00	0:00:03	3 288 K	6 504 K	270	8	534	11
smss.exe	276	SYSTEM	0	00	0:00:00	480 K	188 K	24	5	9	4
rdpclip.exe	212	Administrateur	1	00	0:00:00	388 K	976 K	78	3	13	13
System	4	SYSTEM	0	00	0:00:25	236 K	32 K	376	56	120	4 214
Processus inactif ...	0	SYSTEM	0	98	6:29:54	28 K	0 K	0	1	0	0

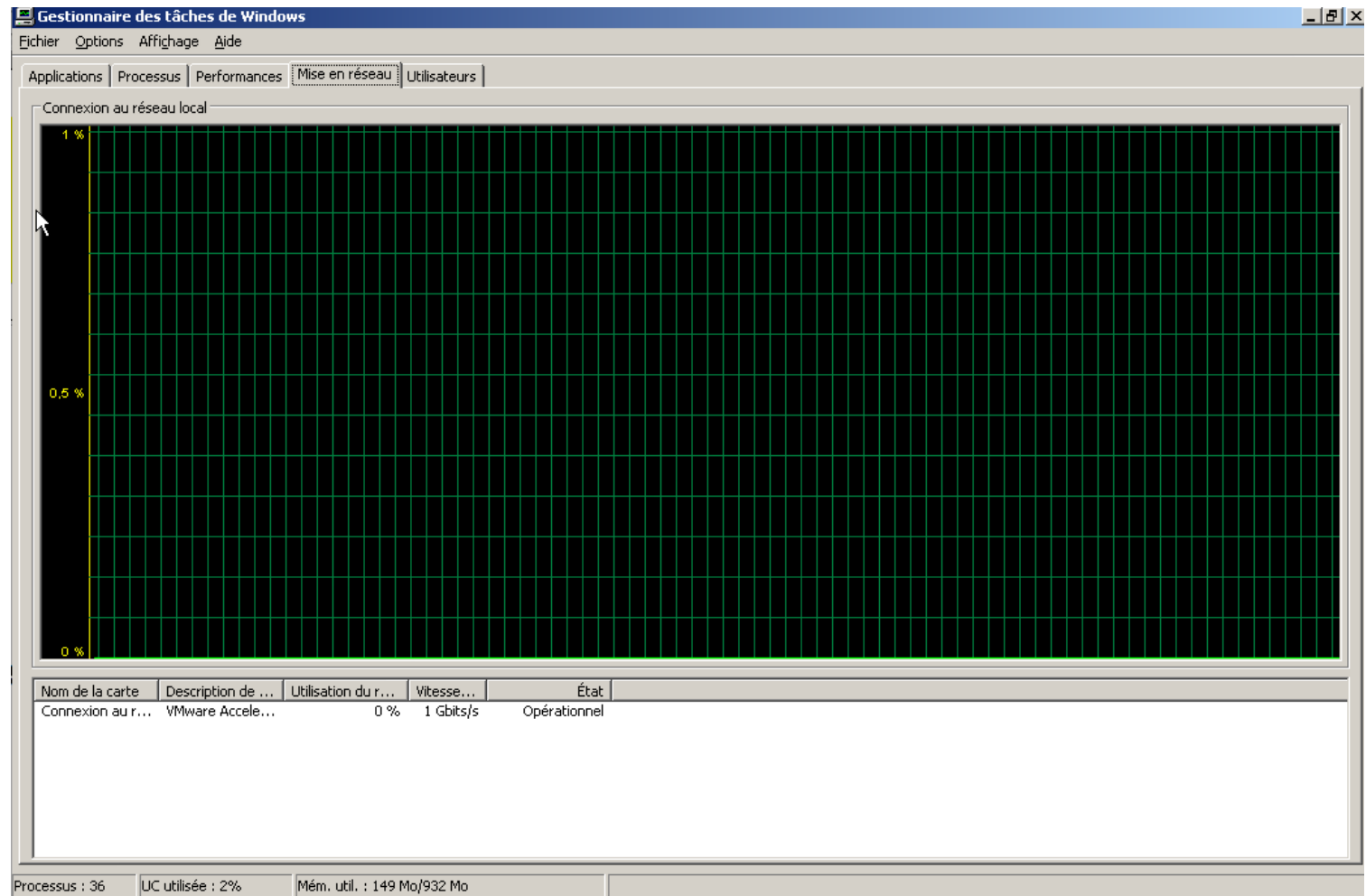
☒ Afficher les processus de tous les utilisateurs

Terminer le processus

Processus : 36 UC utilisée : 4% Mém. util. : 148 Mo/932 Mo

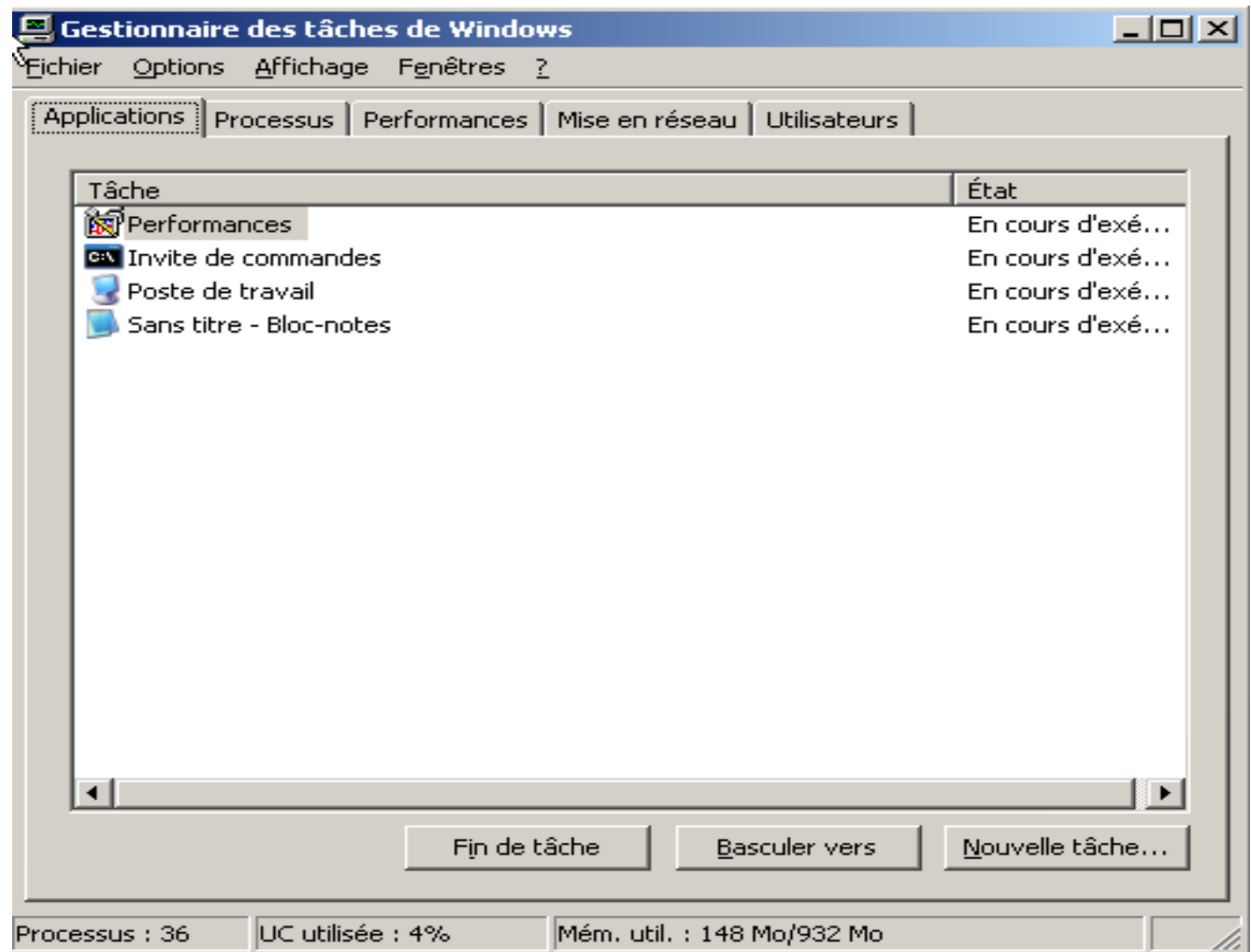
# 2 Les outils d'analyse de Windows

## Onglet mise en réseau



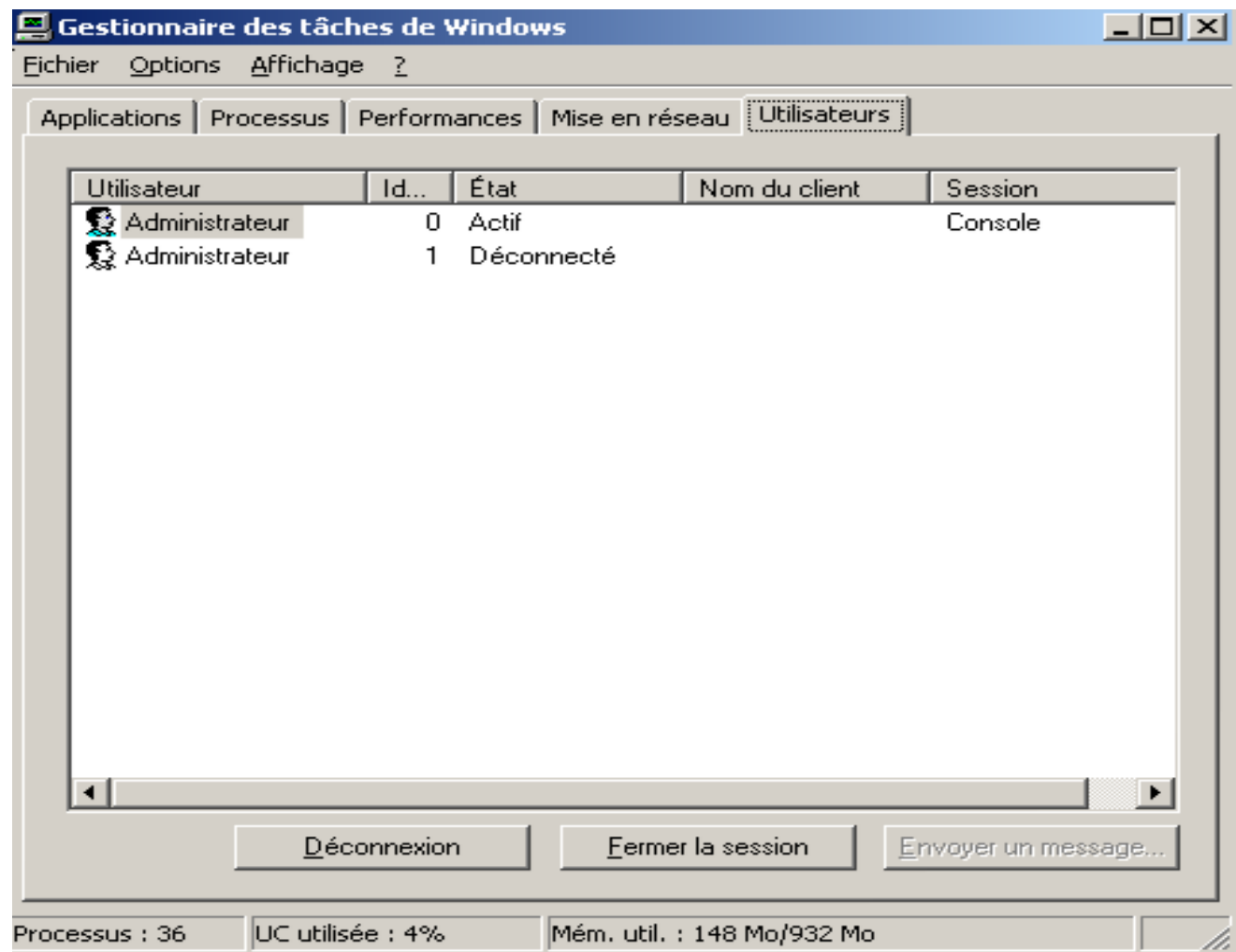
# 2 Les outils d'analyse de Windows

## Onglet applications



# 2 Les outils d'analyse de Windows

## Onglet utilisateurs



## 2 Les outils d'analyse de Windows

### Le moniteur système

Pour lancer le moniteur système il vous suffit de taper ***perfmon*** dans une console ou dans le menu démarrer/exécuter.

Les fonctionnalités offertes par le moniteur dépassent celles du gestionnaire de tâches.

## 2 Les outils d'analyse de Windows

L'affichage est paramétrable.

La sélection des objets mesurés est très souple.

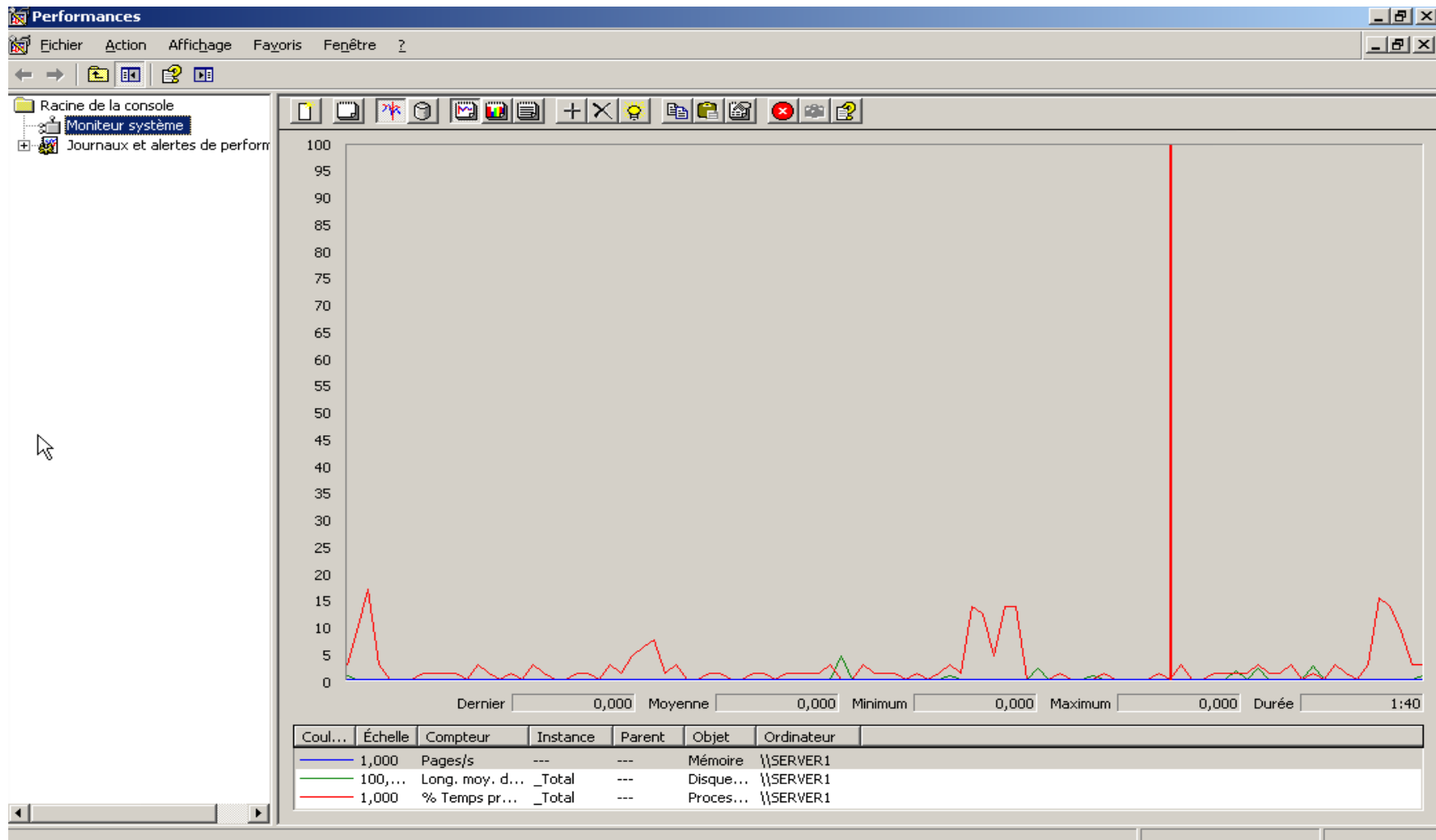
La configuration des compteurs est facile.

On peut sauvegarder les résultats dans différents formats pour une réutilisation ultérieure.

Il est exportable vers d'ordinateurs.

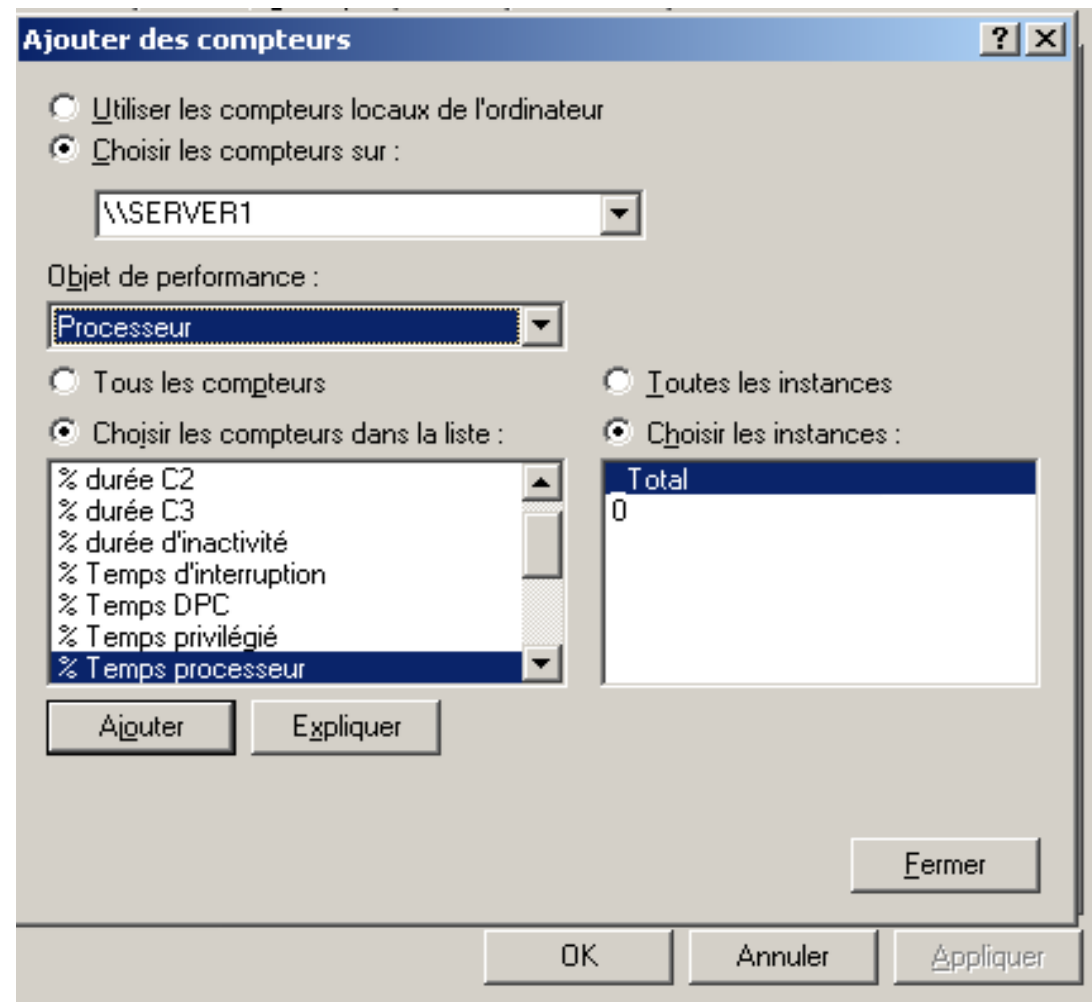
# 2 Les outils d'analyse de Windows

## Vue du moniteur de performances



# 2 Les outils d'analyse de Windows

## Configuration des compteurs





# 2 Les outils d'analyse de Windows

## Journaux et alertes de performance

Il s'agit d'un service Windows offrant des fonctionnalités de journalisation.

On distingue deux types de journaux:

- Les journaux de traces

- Les journaux de compteurs

## 2 Les outils d'analyse de Windows

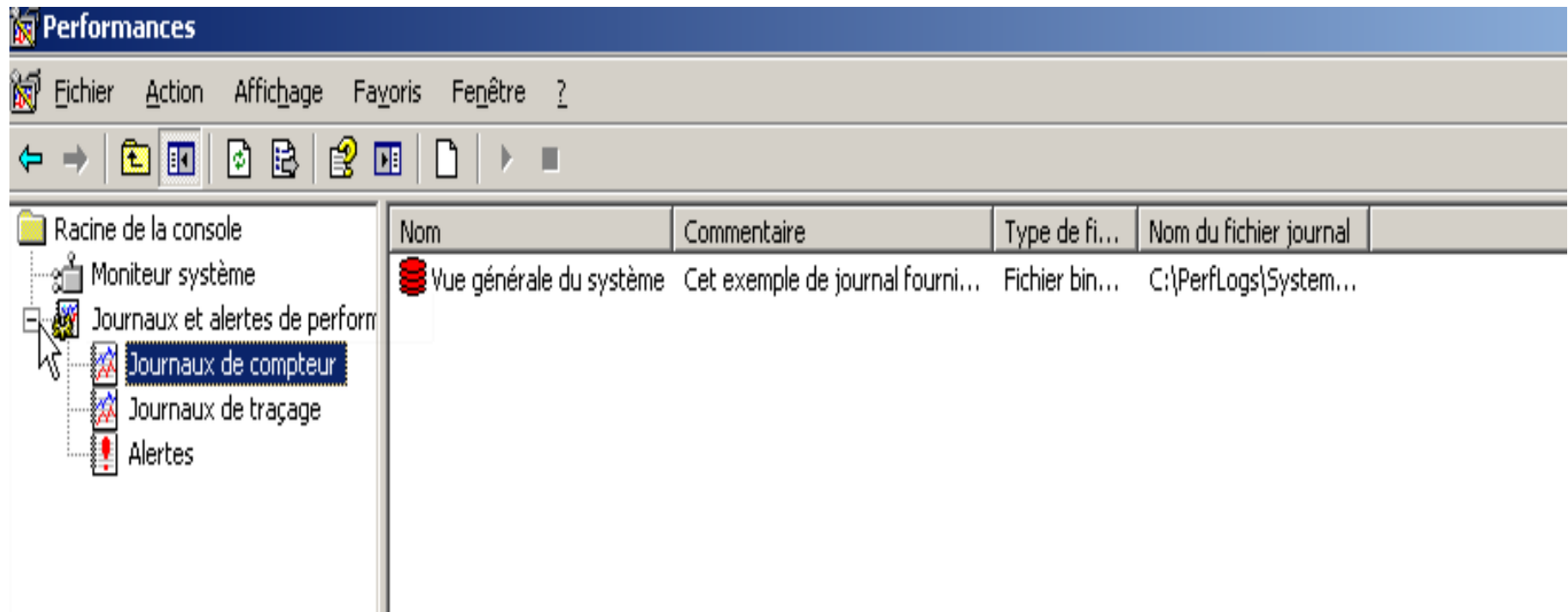
Le journal de compteurs, enregistre des échantillons de données.

Il faut démarrer le journal de compteur pour démarrer l'échantillonnage.

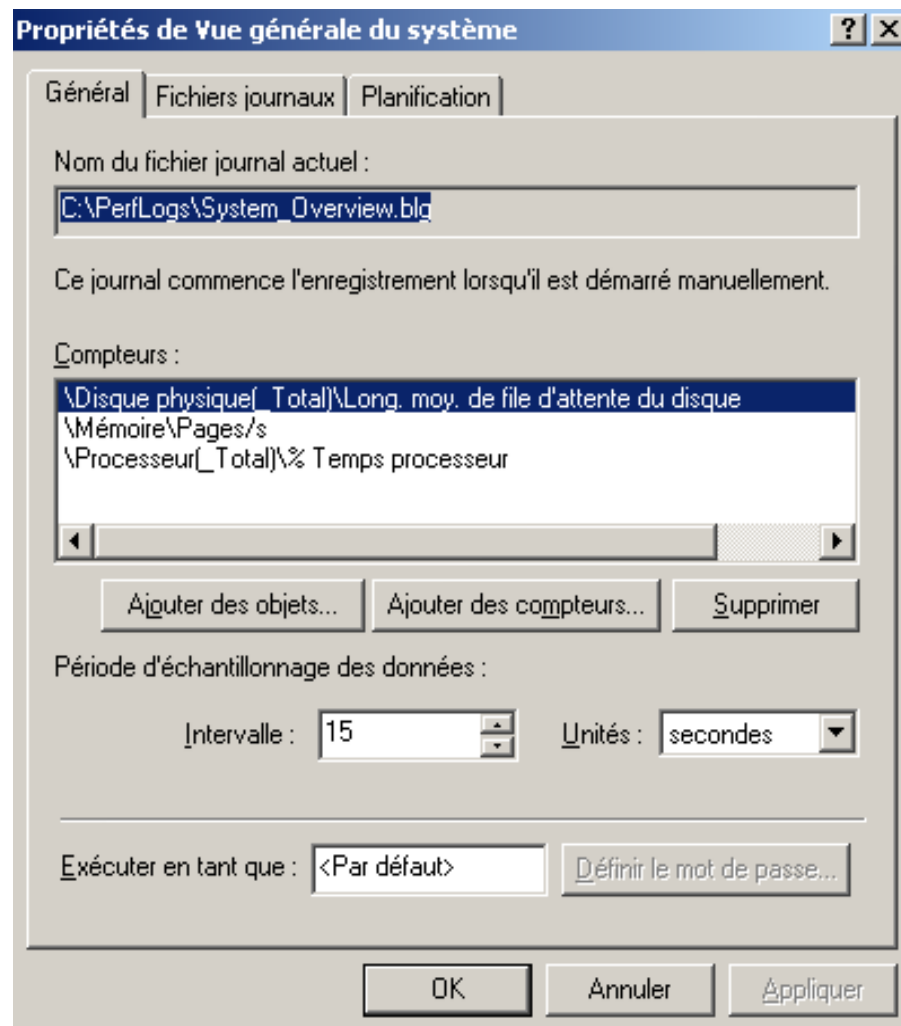
L'échantillonnage se fait en fonction de l'intervalle de temps définit.

On peut exploiter ce journal en le chargeant dans le moniteur système.

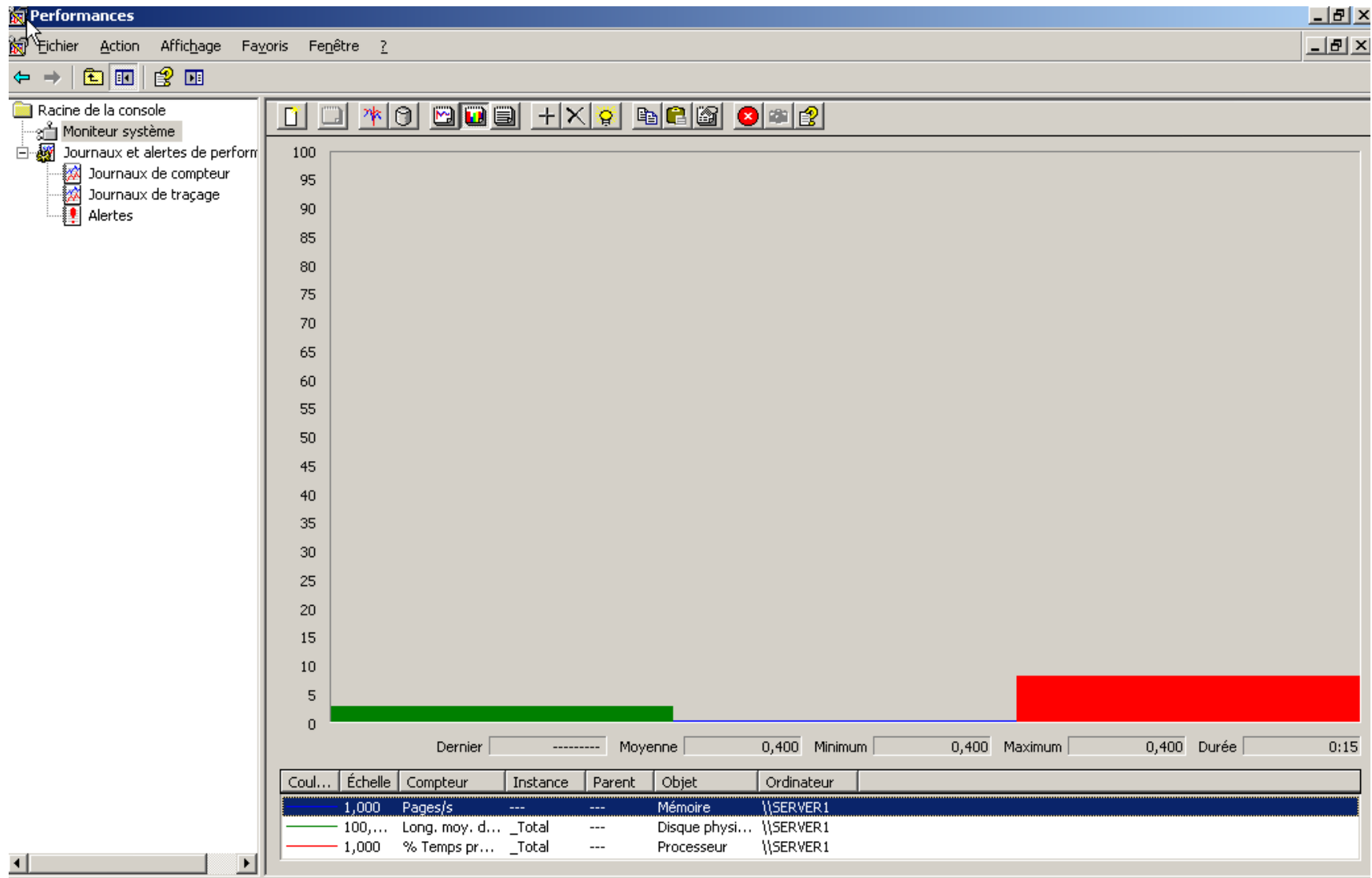
## 2 Les outils d'analyse de Windows



## 2 Les outils d'analyse de Windows



# 2 Les outils d'analyse de Windows



## 2 Les outils d'analyse de Windows

### **Le journal de traçage :**

Il effectue la mesure de performances associée aux événements comme l'activité des threads.

Les données ne sont pas échantillonnées mais mesurées du début à la fin.

C'est pourquoi elles ne sont pas exploitables par le moniteur de performances.

## 2 Les outils d'analyse de Windows

Pour exploiter les résultats il faut utiliser la commande *tracertp* :

*Tracertp inputfile.etl -o outpufile.csv*

```
C:\perflogs>tracertp test_000007.etl -o dumpl.csv
```

```
Entrée
```

```
-----
```

```
Fichier(s) :
```

```
    test_000007.etl
```

```
100.00%
```

```
Sortie
```

```
-----
```

```
Texte (CSV) :
```

```
    dumpl.csv
```

```
L'opération s'est bien déroulée.
```

```
C:\perflogs>
```

# 2 Les outils d'analyse de Windows

Exemple de fichier csv créé :

dumpl.csv - Bloc-notes											
Fichier	Edition	Format	Affichage								
Event Name	Type	TID	Clock-Time	Kernel(ms)	User(ms)	User Data					
EventTrace	En-tête	0x000009F0	128716645270000000	0	0	4096, 33620485, 3790, 1, 128716645309375000, 156250,					
EventTrace	En-tête	0x000009F0	128716645270156250	0	0	65795, 0, 0, 0, 0, 0, 0					
SystemConfig	Processeur	0x000009F0	128716645270312500	15	0	2328, 1, 383, 4096, 65536, "SERVER1", "", 0, 0					
SystemConfig	vidéo	0x000009F0	128716645270312500	15	0	16777216, 1043, 714, 32, 85, "VMware SVGA II", "VMwa					
SystemConfig	PhyDisk	0x000009F0	128716645270468750	30	0	0, 512, 63, 255, 391, 119,					
SystemConfig	PhyDisk	0x000009F0	128716645270468750	30	0	1, 512, 63, 255, 391, 119,					
SystemConfig	PhyDisk	0x000009F0	128716645270468750	30	0	2, 512, 63, 255, 391, 119,					
SystemConfig	LogDisk	0x000009F0	128716645270468750	30	0	32256, 3207823360, 4294967295, 168, 2, "C:",					
SystemConfig	Carte réseau	0x000009F0	128716645270468750	30	0	"VMware Accelerated AMD PCNet Adapter", 65539, 6, "", 16					
SystemConfig	services	0x000009F0	128716645270781250	30	0	"AeLookupSvc", "Service Application Experience Lookup", "svchost.exe",					
SystemConfig	services	0x000009F0	128716645270781250	30	0	"Alerter", "Avertissement", "svchost.exe", 776, 0, 0					
SystemConfig	services	0x000009F0	128716645270781250	30	0	"Browser", "Explorateur d'ordinateurs", "svchost.exe", 812, 0, 0					
SystemConfig	services	0x000009F0	128716645270781250	30	0	"CryptSvc", "Services de cryptographie", "svchost.exe", 812, 0, 0					
SystemConfig	services	0x000009F0	128716645270781250	30	0	"dcomLaunch", "Lanceur de processus serveur DCOM", "svchost.exe", 63					
SystemConfig	services	0x000009F0	128716645270781250	30	0	"dhcp", "Client DHCP", "svchost.exe", 756, 0, 0					
SystemConfig	services	0x000009F0	128716645270781250	30	0	"dmadmin", "Service d'administration du Gestionnaire de disque logique",					
SystemConfig	services	0x000009F0	128716645270781250	30	0	"dmserver", "Gestionnaire de disque logique", "svchost.exe", 812, 0,					
SystemConfig	services	0x000009F0	128716645270781250	30	0	"Dnscache", "Client DNS", "svchost.exe", 756, 0, 0					
SystemConfig	services	0x000009F0	128716645270781250	30	0	"ERSvc", "Service de rapport d'erreurs", "svchost.exe", 1100, 0, 0					
SystemConfig	services	0x000009F0	128716645270781250	30	0	"Eventlog", "Journal des événements", "services.exe", 400, 0, 0					
SystemConfig	services	0x000009F0	128716645270781250	30	0	"EventSystem", "Système d'événements de COM+", "svchost.exe", 812, 0					
SystemConfig	services	0x000009F0	128716645270781250	30	0	"helpsvc", "Aide et support", "svchost.exe", 812, 0, 0					
SystemConfig	services	0x000009F0	128716645270781250	30	0	"lanmanserver", "Serveur", "svchost.exe", 812, 0, 0					
SystemConfig	services	0x000009F0	128716645270781250	30	0	"lanmanworkstation", "Station de travail", "svchost.exe", 812, 0, 0					
SystemConfig	services	0x000009F0	128716645270781250	30	0	"LmHosts", "Assistance TCP/IP NetBIOS", "svchost.exe", 776, 0, 0					
SystemConfig	services	0x000009F0	128716645270781250	30	0	"MSDTC", "Distributed Transaction Coordinator", "msdtc.exe", 1012, 0,					
SystemConfig	services	0x000009F0	128716645270781250	30	0	"Netman", "Connexions réseau", "svchost.exe", 812, 0, 0					
SystemConfig	services	0x000009F0	128716645270781250	30	0	"Nla", "NLA (Network Location Awareness)", "svchost.exe", 812, 0, 0					
SystemConfig	services	0x000009F0	128716645270781250	30	0	"PlugPlay", "Plug-and-Play", "services.exe", 400, 0, 0					
SystemConfig	services	0x000009F0	128716645270781250	30	0	"PolicyAgent", "Services IPSEC", "lsass.exe", 412, 0, 0					
SystemConfig	services	0x000009F0	128716645270781250	30	0	"ProtectedStorage", "Emplacement protégé", "lsass.exe", 412, 0, 0					
SystemConfig	services	0x000009F0	128716645270781250	30	0	"RemoteRegistry", "Accès à distance au Registre", "svchost.exe", 1136					
SystemConfig	services	0x000009F0	128716645270781250	30	0	"Rpcss", "Appel de procédure distante (RPC)", "svchost.exe", 692, 0,					
SystemConfig	services	0x000009F0	128716645270781250	30	0	"SamSs", "Gestionnaire de comptes de sécurité", "lsass.exe", 412, 0,					
SystemConfig	services	0x000009F0	128716645270781250	30	0	"Schedule", "Planificateur de tâches", "svchost.exe", 812, 0, 0					
SystemConfig	services	0x000009F0	128716645270781250	30	0	"seclogon", "Ouverture de session secondaire", "svchost.exe", 812, 0					
SystemConfig	services	0x000009F0	128716645270781250	30	0	"SENS", "Notification d'événement système", "svchost.exe", 812, 0, 0					
SystemConfig	services	0x000009F0	128716645270781250	30	0	"ShellHwDetection", "Détection matériel noyau", "svchost.exe", 812,					
SystemConfig	services	0x000009F0	128716645270781250	30	0	"Spooler", "Spouleur d'impression", "spoolsv.exe", 960, 0, 0					
SystemConfig	services	0x000009F0	128716645270781250	30	0	"SysmonLog", "Journaux et alertes de performance", "smlogsvc.exe", 36					
SystemConfig	services	0x000009F0	128716645270781250	30	0	"TermService", "Services Terminal Server", "svchost.exe", 1392, 0, 0					
SystemConfig	services	0x000009F0	128716645270781250	30	0	"TrkWks", "Client de suivi de lien distribué", "svchost.exe", 812, 0					
SystemConfig	services	0x000009F0	128716645270781250	30	0	"VMTools", "Service VMware Tools", "VMwareService.exe", 1204, 0, 0					
Processus	DCStart	0x00000000	128716645270781250	28699590	0	0x000000E25, 0x000000000, 0x000000000, 0, 0, 0, 0					
Thread	DCStart	0x00000000	128716645270781250	28699590	0	0x000000000, 0x000000000, 0x808948B0, 0x808918B0, 0x000000000, 0x000000000, 0					
Processus	DCStart	0x00000008	128716645270781250	13710	0	0x000000E25, 0x000000004, 0x000000000, 0, 0, 0, "System", 0, 0					
Thread	DCStart	0x00000008	128716645270781250	13710	0	0x000000004, 0x000000008, 0xF78A3000, 0xF78A0000, 0x000000000, 0x000000000, 0					
Thread	DCStart	0x00000010	128716645270781250	0	0	0x000000004, 0x000000010, 0xF78B3000, 0xF78B0000, 0x000000000, 0x000000000, 0					
Thread	DCStart	0x00000014	128716645270781250	15	0	0x000000004, 0x000000014, 0xF78B7000, 0xF78B4000, 0x000000000, 0x000000000, 0					



## 2 Les outils d'analyse de Windows

### **Les alertes :**

La configuration des alertes, permet de définir des seuils d'alertes, associés à une action en cas de dépassement du seuil.

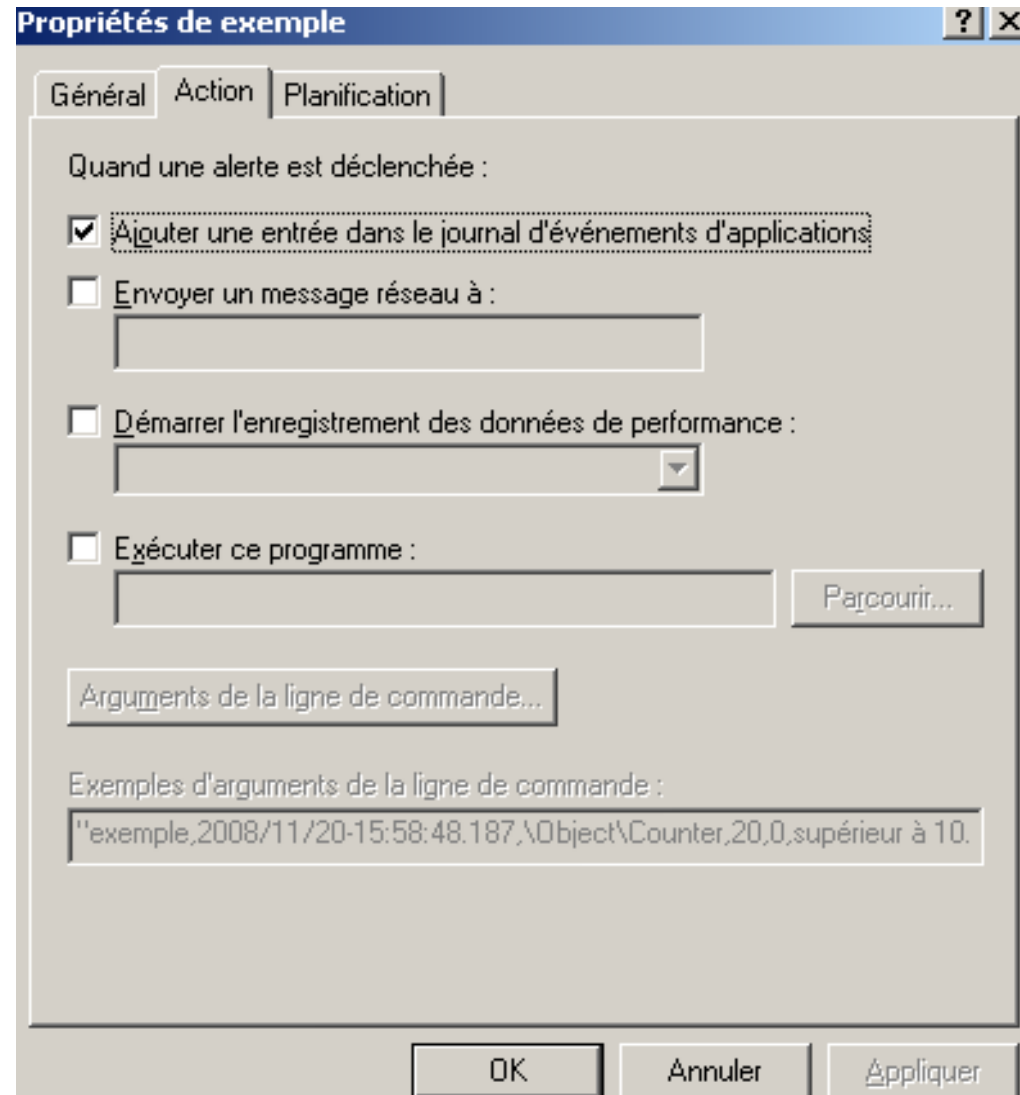
On peut par exemple envoyer un courrier, inscrire l'alerte dans le journal d'application.

## 2 Les outils d'analyse de Windows

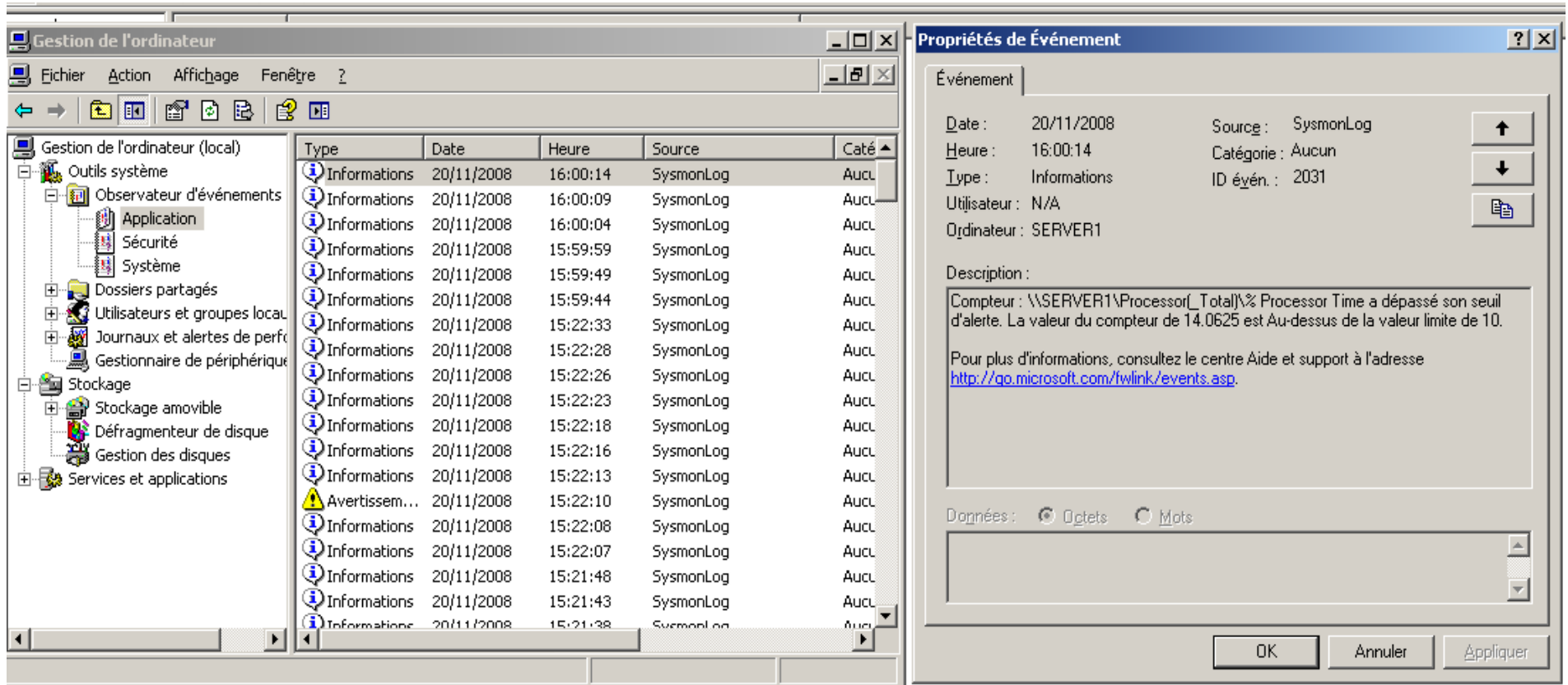
The image shows a Windows dialog box titled "Propriétés de exemple". It has three tabs: "Général", "Action", and "Planification". The "Général" tab is selected. The dialog contains the following elements:

- A text box with the text: "Cette alerte commence lorsqu'elle est démarrée manuellement."
- A label "Commentaire :" followed by a text input field.
- A label "Compteurs :" followed by a list box containing the text "\\SERVER1\\Processeur[\_Total]\\% Temps processeur".
- A label "Avertir si la valeur est :" followed by a dropdown menu showing "supérieure à".
- A label "Limite :" followed by a text input field containing "0".
- Two buttons: "Ajouter..." and "Supprimer".
- A label "Période d'échantillonnage des données :".
- A label "Intervalle :" followed by a spin box showing "5".
- A label "Unités :" followed by a dropdown menu showing "secondes".
- A label "Exécuter en tant que :" followed by a text input field containing "<Par défaut>".
- A button "Définir le mot de passe...".
- At the bottom, three buttons: "OK", "Annuler", and "Appliquer".

## 2 Les outils d'analyse de Windows



# 2 Les outils d'analyse de Windows



# 3 Les goulets d'étranglement

1 Concepts d'analyse

2 les outils d'analyse de Windows

3 Les goulets d'étranglement

# 3 Les goulets d'étranglement

À l'aide des outils précédent, vous allez pouvoir établir une valeur de référence.

Pour établir une valeur de référence il faut collecter assez d'informations sur une longue période.

Il faut aussi que cette collecte s'effectue dans des conditions normales d'activité.

Cette référence sera un indicateur et vous permettra d'établir des seuils d'alerte.

# 3 Les goulets d'étranglement

Une fois la collecte des données effectuée vous pourrez établir des niveaux d'utilisation du système, par exemple :

Bas  
Moyen  
Élevé  
Critique

# 3 Les goulets d'étranglement

Si la performance chute il y a peut-être présence d'un goulet d'étranglement.

Toute la structure de collecte de données que vous avez établie vous vient en aide à ce moment.

S'agit-il d'un état temporaire ?

Le phénomène se répète-t'il ?

À quelle fréquence ?



# 3 Les goulets d'étranglement

Par exemple vous pourrez détecter un goulet d'étranglement au niveau du processeur en observant le comportement des threads.

L'analyse d'un système est délicate et ardue, il ne faut pas tirer de conclusion hâtive d'un phénomène.

Par exemple si le processeur est occupé à 99% mais qu'aucune file d'attente ne s'est formée, alors il n'y a pas de goulet d'étranglement, il s'agit juste d'un pic de charge.

# 3 Les goulots d'étranglement

Une bonne exploitation de ces outils d'analyse, permettra la détection des problèmes, et vous sera une aide, quant à la décision de faire évoluer le système :

- Ajout de mémoire

- Ajout de disque

- Mise en cluster

# 3 Les goulots d'étranglement

**Analyse en fonction des rôles :**

Vous ne concentrerez pas vos efforts d'analyse sur les mêmes compteurs en fonction des rôles de votre serveur.

Rôle	Observations
Contrôleur de domaine	processeur, mémoire, réseau, disques
Serveur de fichiers	mémoire, réseau, disques
Serveur d'applications	mémoire, processeur
Serveur de base de données	disques, processeur