Analyse du réseau

M. EL AOUN

A24

Outline

1 Introduction

Introduction

- Types de problèmes :
  - Problèmes matériels
  - Charge excessive (processeur, mémoire, E/S)
- Supervision continue
  - Vérifier régulièrement l'état du réseau
  - Se familiariser avec les outils de gestion du réseau
  - Créer un modèle de référence des états normaux du réseau.
- Gestion d l'historique
  - Base de données
  - Agent SNMP

Analyse interne

- Processus
  - Processus en cours d'exécution (actif)
  - Processus en attente (inactif : attendant leur tour ou bloqués)
- Mémoire
  - Réelle
  - Virtuelle
- E/S (Input/Output)
  - Stockage
  - Réseau

Quelques indicateurs

- Processeur insuffisant
  - Nombre de processus en attente d'exécution toujours élevé
  - Utilisation élevée du processeur (charge moyenne)
- Mémoire insuffisante
  - Très peu de mémoire disponible
  - Beaucoup de processus bloqués
  - Nombre élevé de transferts de blocs

Analyse sous Unix

- Plusieurs outils :
  - top
  - lsof
  - netstat
  - tcpdump
  - wireshark
  - iperf

top

- Outil d'analyse de performances standard pour les environnements Unix/Linux
- Affiche périodiquement une liste de statistiques de performances système :
  - Utilisation du processeur
  - Utilisation de la mémoire RAM et SWAP
  - Charges moyennes (Utilisation du processeur)
  - Information par processus

top

- Exemple

```
top - 09:57:06 up 1 day, 23:13,  1 user,  load average: 0.08, 0.03, 0.01
Tasks: 196 total,   1 running, 146 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0.4 us,  0.0 sy,  0.0 ni, 99.6 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0
KiB Mem : 16240044 total, 12111520 free,  2081080 used,  2047444 buff/cache
KiB Swap:  2097148 total,  2097148 free,        0 used. 13820928 avail Mem
```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
992	tomcat	20	0	9981472	1.355g	16832	S	2.3	8.8	11:03.09	java
11	root	20	0	0	0	0	I	0.3	0.0	0:24.09	rcu_sch+
738	avahi	20	0	47476	4076	3380	S	0.3	0.0	1:04.76	avahi-d+
7781	**esp**	**20**	**0**	**44080**	**4152**	**3476**	**R**	**0.3**	**0.0**	**0:00.21**	**top**
1	root	20	0	225412	9076	6624	S	0.0	0.1	0:14.10	systemd
2	root	20	0	0	0	0	S	0.0	0.0	0:00.01	kthreadd
3	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	rcu_gp

top

- Information par processus (colonnes les plus intéressantes)
  - PID : ID du processus
  - USER : utilisateur (propriétaire) du processus
  - %CPU : pourcentage d'utilisation du processeur par le processus depuis le dernier rapport
  - %MEM : pourcentage de mémoire physique (RAM) utilisée par le processus
  - TIME : temps processeur total utilisé par le processus depuis son démarrage
- Quelques commandes
  - -f : Ajoute ou supprime des colonnes
  - -F : Spécifie sur quelle colonne s'effectue le tri
  - -u : Spécifie un utilisateur
  - -k : Spécifie le processus à tuer (arrêter)

netstat

- Affiche des informations sur :
- Les connexions réseau
- Les tables de routage
- Les statistiques des interfaces (NIC)
- Quelques commandes :
  - -n: Affiche les adresses, ports et ID utilisateurs en format numérique
  - -r : Table de routage
  - -s : Statistiques par protocole
  - -i : Statut des interfaces
  - -l : Sockets à l'écoute
  - –tcp, –udp : Spécifie le protocole

netstat

- Exemples :

lsof

- **lsof** est particulièrement utile parce que sous Unix, tout est fichier : sockets unix, sockets ip, répertoires, etc.
- Permet d'associer les fichiers ouverts par :
  - -p : PID (ID Processus)
  - -i : Adresse réseau (protocole:port)
  - -u : Utilisateur

```
COMMAND     PID  TID           USER   FD      TYPE             DEVICE SIZE/OFF       NODE NAME
systemd       1                root  cwd   unknown                                      /proc/1/cwd (readlink: Permission denied)
systemd       1                root  rtd   unknown                                      /proc/1/root (readlink: Permission denied)
systemd       1                root  txt   unknown                                      /proc/1/exe (readlink: Permission denied)
systemd       1                root NOFD                                                /proc/1/fd (opendir: Permission denied)
kthreadd      2                root  cwd   unknown                                      /proc/2/cwd (readlink: Permission denied)
kthreadd      2                root  rtd   unknown                                      /proc/2/root (readlink: Permission denied)
kthreadd      2                root  txt   unknown                                      /proc/2/exe (readlink: Permission denied)
kthreadd      2                root NOFD                                                /proc/2/fd (opendir: Permission denied)
rcu_gp        3                root  cwd   unknown                                      /proc/3/cwd (readlink: Permission denied)
rcu_gp        3                root  rtd   unknown                                      /proc/3/root (readlink: Permission denied)
rcu_gp        3                root  txt   unknown                                      /proc/3/exe (readlink: Permission denied)
```

tcpdump

- Affiche les entêtes de paquets reçus par une interface donnée. En option, permet de filtrer à l'aide d'expressions booléennes.
- Permet d'enregistrer des informations dans un fichier pour analyse ultérieure.
- Nécessite des droits d'administrateur (root).
- Quelques commandes :
  - -i : Spécifie l'interface (ex : -i eth0)
  - -l : Place la ligne de sortie standard (stdout) en tampon (visualisation au fil de la capture)
  - -n : Pas de conversion des adresses en noms (pas de DNS)
- - Utilisant les opérateurs 'AND', 'OR', 'NOT'

Wireshark

- Wireshark est un analyseur de paquets graphique basé sur libpcap, la bibliothèque que tcpdump utilise pour capturer et stocker des paquets