Supervision

Sommaire

Introduction

Supervision

“Know your infra”

- Prévenir
- Guérir
- Justifier
- Optimiser

Principe de la supervision

- supervision réseau
- supervision système
- supervision applicative
- exécution de commandes
- alerte
- vue d'ensemble
- tableaux de bord

Journaux systèmes

Introduction

- Depuis le démarrage jusqu'à l'arrêt de la machine, enregistrement d'informations en provenance du noyau, des services et de différents programmes utilisateurs.
- Intérêt :
  - Vérification du bon fonctionnement du système et des services
  - Enregistrement des anomalies (dysfonctionnement, erreurs, warning)
  - Une source d'information importante pour la mise au point et le diagnostic.

Syslog

```
Apr  6 09:07:28 workine sshd[9424]: Accepted publickey for tom from 192.168.10.129 port 45645 ssh2
Apr  6 09:07:28 workine sshd[9424]: pam_unix(sshd:session): session opened for user tom by (uid=0)
```

- Format utilisé pour l'écriture de journaux systèmes.
- Protocole permettant l'envoi et la réception de messages d'évènements systèmes.
- Démon de traitements de MES :
  - rsyslogd
- Tests avec logger :

```
$ logger -p user.notice msg de test
$ tail /var/log/syslog

Mar 13 15:44:16 debian postfix/master[3835]: daemon started -- version 2.3.8, configuration /etc/
      postfix
Mar 13 15:46:26 debian tom: msg de test
```

Configuration

- Elle se trouve dans le fichier */etc/rsyslogd.conf* et */etc/rsyslogd.d*
- Les messages sont sélectionnés suivant une *facility* et une *priorité*.
- A cette sélection est appliqué une action, généralement l'envoi vers un fichier de log donné.

authpriv	système d'authentification et de sécurité
cron	tâches planifiées
dameon	services
kern	kernel
local0 $\sim$ 7	messages utilisateur
mail	système de messagerie

TABLE – Facilities

emerg	système inutilisable
crit	réponse nécessaire rapidement
err	erreur sérieuse
warn	avertissement
notice	remarque
info	information de fonctionnement
debug	information de déboggage

TABLE – Priorité

Configuration

```
auth,authpriv.*                 /var/log/auth.log
*.*;auth,authpriv.none          -/var/log/syslog
daemon.*                        -/var/log/daemon.log
*.crit                          /dev/console
*.*                             @loghost.domaine.org
*.emerg                         *
```

Rotation des logs

- L'administration des fichiers de log est assurée par l'utilitaire *logrotate*.
- Celui-ci est chargé de repérer les logs à remettre à zéro, de gérer les anciens logs (archivage, suppression, envoi par mail, ...) et de redémarrer l'application cliente, au besoin :

```
/var/log/apache2/*.log {
  weekly
  missingok
  rotate 52
  compress
  notifempty
  create 640 root adm
  sharedscripts
  postrotate
  if [ -f /var/run/apache2.pid ]; then
  /usr/sbin/apache2ctl graceful > /dev/null
  fi
  endscript
}
```

Logcheck

- Logcheck est un logiciel d'analyse de journaux.
- Il peut détecter certains évènements, et en ignorer d'autres.
- Il génère un rapport des éléments détectés et l'envoie par mail
- Architecture :
  - 3 niveaux de vigilance (workstation, server, paranoid)
  - Les éléments sont classés en 2 catégories ("system events" et "security violations").
  - les éléments à détecter sont dans /etc/logcheck/cracking.d et /etc/logcheck/violations.d
  - les éléments de type "system events" à ignorer sont dans /etc/logcheck/ignore.d.LEVEL
  - les éléments de type "security violations" à ignorer sont dans /etc/logcheck/violations.ignore.d

Introduction

Logwatch permet de générer des rapports à partir des logs système.
Intéressant, si on se discipline à les lire.

```
(<5036>tom@workine)sudo logwatch --range Today --detail=high                    (0)(~)( 3:56
      mer. 13)

 ################### Logwatch 7.3.6 (05/19/07) ####################
        Processing Initiated: Wed Apr 13 15:57:08 2011
        Date Range Processed: today
                              ( 2011-Apr-13 )
                              Period is day.
        Detail Level of Output: 10
        Type of Output/Format: stdout / text
        Logfiles for Host: workine
 ################################################################

 ---------- clam-update Begin ----------

 The ClamAV update proce
 ...
  ---------- Cron Begin ----------



 Commands Run:
    User logcheck:
          if [ -x /usr/sbin/logcheck ]; then nice -n10 /usr/sbin/logcheck; fi: 16 Time(s)
    User root:
          cd / && run-parts --report /etc/cron.hourly: 16 Time(s)
```

Journaux systèmes

Introduction

- Depuis le démarrage jusqu'à l'arrêt de la machine, enregistrement d'informations en provenance du noyau, des services et de différents programmes utilisateurs.
- Intérêt :
  - Vérification du bon fonctionnement du système et des services
  - Enregistrement des anomalies (dysfonctionnement, erreurs, warning)
  - Une source d'information importante pour la mise au point et le diagnostic.

Syslog

```
Apr  6 09:07:28 workine sshd[9424]: Accepted publickey for tom from 192.168.10.129 port 45645 ssh2
Apr  6 09:07:28 workine sshd[9424]: pam_unix(sshd:session): session opened for user tom by (uid=0)
```

- Format utilisé pour l'écriture de journaux systèmes.
- Protocole permettant l'envoi et la réception de messages d'évènements systèmes.
- Démon de traitements de MES :
  - rsyslogd
- Tests avec logger :

```
$ logger -p user.notice msg de test
$ tail /var/log/syslog

Mar 13 15:44:16 debian postfix/master[3835]: daemon started -- version 2.3.8, configuration /etc/
      postfix
Mar 13 15:46:26 debian tom: msg de test
```

Configuration

- Elle se trouve dans le fichier */etc/rsyslogd.conf* et */etc/rsyslogd.d*
- Les messages sont sélectionnés suivant une *facility* et une *priorité*.
- A cette sélection est appliqué une action, généralement l'envoi vers un fichier de log donné.

authpriv	système d'authentification et de sécurité
cron	tâches planifiées
dameon	services
kern	kernel
local0 $\sim$ 7	messages utilisateur
mail	système de messagerie

TABLE – Facilities

emerg	système inutilisable
crit	réponse nécessaire rapidement
err	erreur sérieuse
warn	avertissement
notice	remarque
info	information de fonctionnement
debug	information de déboggage

TABLE – Priorité

Configuration

```
auth,authpriv.*                 /var/log/auth.log
*.*;auth,authpriv.none          -/var/log/syslog
daemon.*                        -/var/log/daemon.log
*.crit                          /dev/console
*.*                             @loghost.domaine.org
*.emerg                         *
```

Rotation des logs

- L'administration des fichiers de log est assurée par l'utilitaire *logrotate*.
- Celui-ci est chargé de repérer les logs à remettre à zéro, de gérer les anciens logs (archivage, suppression, envoi par mail, ...) et de redémarrer l'application cliente, au besoin :

```
/var/log/apache2/*.log {
  weekly
  missingok
  rotate 52
  compress
  notifempty
  create 640 root adm
  sharedscripts
  postrotate
  if [ -f /var/run/apache2.pid ]; then
  /usr/sbin/apache2ctl graceful > /dev/null
  fi
  endscript
}
```

Logcheck

- Logcheck est un logiciel d'analyse de journaux.
- Il peut détecter certains évènements, et en ignorer d'autres.
- Il génère un rapport des éléments détectés et l'envoie par mail
- Architecture :
  - 3 niveaux de vigilance (workstation, server, paranoid)
  - Les éléments sont classés en 2 catégories ("system events" et "security violations").
  - les éléments à détecter sont dans /etc/logcheck/cracking.d et /etc/logcheck/violations.d
  - les éléments de type "system events" à ignorer sont dans /etc/logcheck/ignore.d.LEVEL
  - les éléments de type "security violations" à ignorer sont dans /etc/logcheck/violations.ignore.d

Introduction

Logwatch permet de générer des rapports à partir des logs système.
Intéressant, si on se discipline à les lire.

```
(<5036>tom@workine)sudo logwatch --range Today --detail=high                    (0)(~)( 3:56
      mer. 13)

 ###################### Logwatch 7.3.6 (05/19/07) ######################
        Processing Initiated: Wed Apr 13 15:57:08 2011
        Date Range Processed: today
                              ( 2011-Apr-13 )
                              Period is day.
        Detail Level of Output: 10
        Type of Output/Format: stdout / text
        Logfiles for Host: workine
 ##########################################################################

 --------------------- clam-update Begin ------------------------

 The ClamAV update proce
 ...
  ------------------------ Cron Begin -------------------------



 Commands Run:
    User logcheck:
          if [ -x /usr/sbin/logcheck ]; then nice -n10 /usr/sbin/logcheck; fi: 16 Time(s)
    User root:
          cd / && run-parts --report /etc/cron.hourly: 16 Time(s)
```

SNMP

Qu'est ce que c'est ?

Un protocole

- simple
- standardisé

d'interrogation et de fourniture de renseignements

Architecture

- un *manager*, qui envoient les requêtes
- des agents sur chaque équipement (udp161), répondant aux requètes
- et pouvant envoyer des alertes (trap)

Les versions

1 obsolète

2c plus “performante”

3 plus “sécurisée” mais rarement implémentée

Sécurité

SNMP peut manipuler des données sensibles et réaliser des manipulations critiques.

- En clair
- notion de *communauté*
- communauté *public* par défaut.

Simple

- protocole UDP (et ses défauts)
- 5 messages : get-request, get-next-request, set-request, get-response, trap

Installation et paramétrage

- paquets *net-snmp* et *net-snmp-utils*
- service *snmpd*
- fichier de configuration */etc/snmp/snmpd.conf* :

```
rocommunity   mycommunity 192.168.10.0/24
rwcommunity mycommunity localhost
```

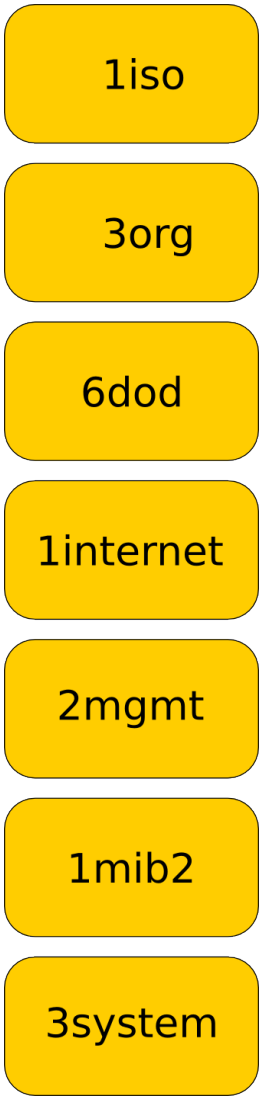
À vous de jouer : installez et paramétrez le service snmp. Amusez-vous à l'interroger avec *snmpwalk*. Facile à exploiter non ?

MIB

Base de donnée contenant les informations manipulables via SNMP

- structure arborescente
- chaque info est identifiée (OID)
- la plus courante est *MIB-II*

MIB et notation ASN.1



.iso.org.dod.internet.mgmt.mib−2.system.
sysUpTime

DISMAN−EVENT−MIB::sysUpTimeInstance

.1.3.6.1.2.1.1.3.0

Au boulot : Rajoutez à l'arbre ci-dessus la branche "machine à café" dont la

Les commandes

snmp(bulk)walk permet de parcourir tout ou partie d'un arbre.

snmptranslate permet d'obtenir une description à partir d'un oid, et réciproquement

Options communes :

- -v 2c
- -c community

Un peu d'exploration

1. trouvez la valeur de *.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime*
2. trouvez la description complète de *.iso.org.dod.internet.mgmt.mib-2.system.sysUpTime*
3. trouvez la valeur, et le type d'info qui se cache derrière l'OID .1.3.6.1.2.1.1.4.0
4. trouvez quelle branche (valeur numérique et textuelle) stocke la configuration ip des interfaces réseau

MRTG

MRTG

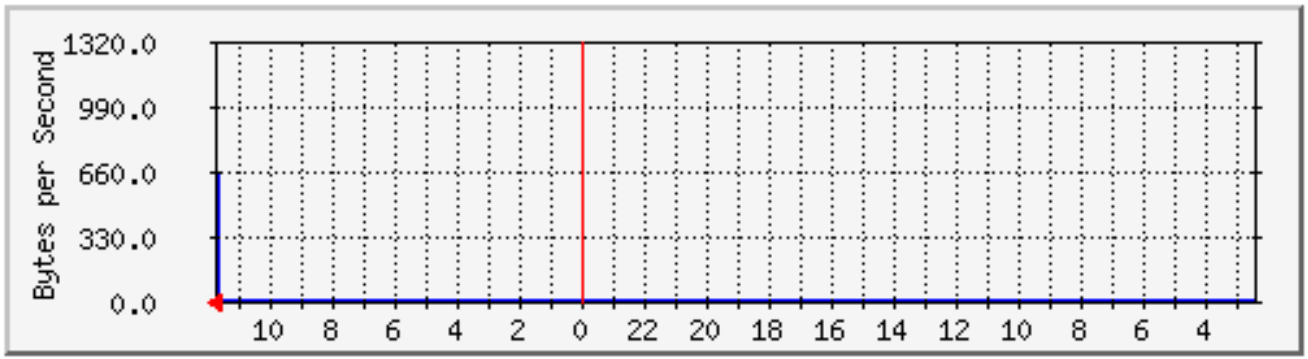
C'est un outil utilisant *SNMP* pour récupérer les statistiques d'utilisation d'un (ou plusieurs) routeur

Traffic Analysis for 10 -- rotamfrgw01

System: rotamfrgw01 in Hsinchu,Taiwan
Maintainer: support@zyxel.com.tw
Description: br0
ifType: ethernetCsmacd (6)
ifName:
Max Speed: 1250.0 kBytes/s

The statistics were last updated **Thursday, 26 September 2013 at 11:45**, at which time '**rotamfrgw01**' had been up for **2 days, 2:01:46.**

`Daily' Graph (5 Minute Average)



Max Average Current

Installation et utilisation

1. yum install mrtg
2. service httpd reload
3. cfgmaker --global 'WorkDir: /var/www/mrtg' --output /etc/mrtg/mrtg.cfg COMMUNITY@ROUTERADDRESS
4. indexmaker --output=/var/www/mrtg/index.html /etc/mrtg/mrtg.cfg
5. firefox http :// localhost / mrtg

Conclusion

Conclusion

La supervision est un outil indispensable à la gestion optimale d'une infrastructure IT
Nagios et snmp permettent de mettre en place une solution de supervision exhaustive, bon marché et efficace.
Si vous souhaitez aller plus loin :

- snmp
- mib explorer
- Réseau informatique, Supervision et Administration par François Pignet, Éd Dunod
- Shinken, nagios contender

Merci de votre attention.

Licence

CC-BY-NC-SA