Supervision

Utilisation de Check-MK

Réseau Min2Rien
Journée Thématique « retour d'expériences » - 13/02/2014

NICOLAS JAMIN – Administrateur Système – DSI de l'Académie de LILLE

CC BY NC SA

Plan

- Présentation
- Fonctionnement / Configuration
- Création de scripts (Présentation et exemple)
- Utilisation / Capture d'écran
- Livestatus / Multisite

- Check-MK : add-on de supervision écrit en python

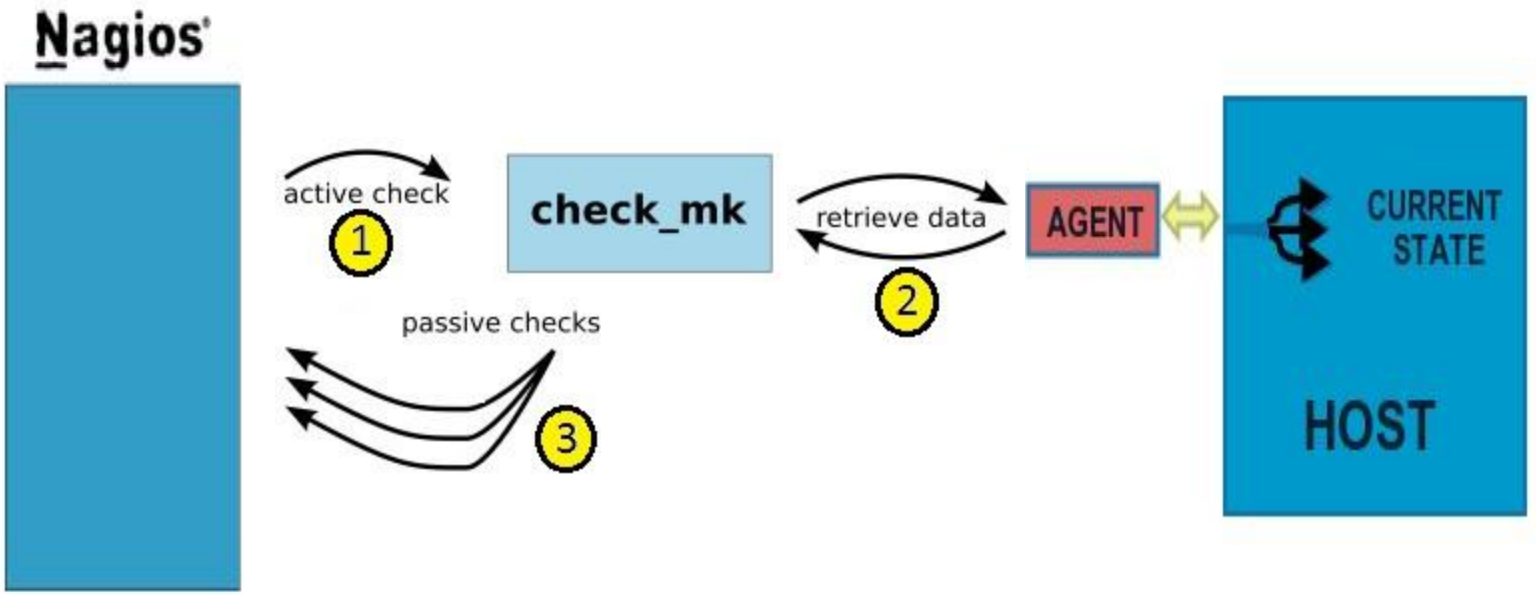
- Nagios utilise des plugins de type actif
  - ✓ 1 plugin = 1 service
  - ✓ Exécution côté Nagios
    - Exemple: check_disk = test de l'espace disque

- Check-MK utilise des plugins de type passif
  - ✓ 1 plugin ~ 30 tests de base
  - ✓ Exécution côté Client
    - Exemple: check_mk = check_disk + check_mem + check_ps + …

- Forte baisse du taux d'utilisation des CPUs sur Nagios grâce à Check-MK

- Remplace les plugins de type NRPE, NSCLIENT ++

Fonctionnement



- Fichier main.mk
  - ✓ Contient la configuration générale (seuil d'alerte, exclusions des services …)
    - Inventory_df_exclude_mountpoints = ['/dev','/mnt/vzsnap0']
    - Filesystem_default_level['levels'] = (90.0, 95.0)

- Fichier tcp_hosts.mk
  - ✓ Contient les hosts et hostgroups des serveurs auxquels ils appartiennent.
    - template124.expr.in.ac-lille.fr|linux|apt|openvz|ubuntu12

- Fichier hostgroups.mk
  - ✓ Contient la définition des hostgroups.
    - ('Serveurs Ubuntu 12.04', ['ubuntu12'], ALL_HOSTS),

Configuration (sur le serveur NAGIOS)

- Plus aucune configuration côté Nagios Core
  - ~~/etc/nagios/host.cfg,~~ ~~/etc/nagios/hostgroup.cfg~~ …
- Check-MK s'occupe lui-même de la génération des fichiers de configuration de Nagios
- Fonctionne en parallèle de Nagios Core (toujours la possibilité de réaliser des check actifs)
- Interfaces de type Centreon … n'ont plus lieu d'être

- Agent Multiplateforme (Linux, Windows)
  - ✓ Linux: agent + xinetd à installer (TCP port 6556)
  - ✓ Windows : agent

- Pas de configuration ni de paramétrage

- Binaire python qui englobe tous les services à monitorer
  - ✓ sous linux /usr/bin/check_mk_agent

Supervision: Utilisation de Check-MK

Configuration (sur le client) – Exemple de sortie de l'agent

```
<<<check_mk>>>
Version: 1.2.2p2
AgentOS: linux
PluginsDirectory: /usr/lib/check_mk_agent/plugins
LocalDirectory: /usr/lib/check_mk_agent/local
AgentDirectory: /etc/check_mk
<<<df>>>
/dev/simfs   simfs     4194304    637632   3556672      16% /
<<<nfsmounts>>>
<<<mounts>>>
/dev/simfs / simfs rw,relatime 0 0
<<<ps>>>
(root,23464,1636,0.0) init
(root,0,0,0.0) [kthreadd/1209]
(root,0,0,0.0) [khelper/1209]
(root,49280,1088,0.0) /usr/sbin/sshd
(root,21092,904,0.0) cron
(syslog,12464,788,0.0) /sbin/syslogd -u syslog
(root,19544,988,0.0) /usr/sbin/xinetd -pidfile /var/run/xinetd.pid -stayalive -inetd_compat -inetd_ipv6
(root,10772,1548,0.0) /bin/bash /usr/bin/check_mk_agent
(root,10008,1080,0.0) less
(root,14996,1072,0.0) ps ax -o user,vsz,rss,pcpu,command --columns 10000
(root,8340,772,0.0) sed -e 1d -e s/ *\([^ ]*\) *\([^ ]*\) *\([^ ]*\) *\([^ ]*\) */(\1,\2,\3,\4) /
(root,70616,3312,0.0) sshd: root@pts/0
(root,19528,2304,0.0) -bash
(root,42288,1688,0.0) /usr/sbin/monit -c /etc/monit/monitrc -s /var/lib/monit/monit.state
<<<mem>>>
MemTotal:         524288 kB
MemFree:          331468 kB
Cached:           164972 kB
Active:           144856 kB
Inactive:          24284 kB
Active(anon):       1340 kB
```

- Des services supplémentaires peuvent être monitorés
- Possibilité de créer des scripts locaux
- Langage de programmation
  - ✓ Python
  - ✓ Perl
  - ✓ Bash
  - ✓ …
- Pas de limitation sur le type et le nombre de tests
- Norme de sortie à respecter

- Vérification du commit des dépôts mercurial
  - Recherche des dépôts

```
#!/bin/bash

DEPOTFILE="/var/run/mercurial-depot"
date=`date "+%Y%m%d"`

function cherche_depot
{
     local datefich
     if [[ -f $DEPOTFILE ]]; then
             datefich=`head -n 1 $DEPOTFILE`
     else
             datefich=""
     fi
     if [[ "$datefich" != "$date" ]]; then
         updatedb
         date "+%Y%m%d" > $DEPOTFILE
         locate --regex "/\.hg$" | sed 's/.hg$//' | grep -v "^/home" | grep -v "^/DOMAINE" | grep -v "^/root" >> $DEPOTFILE
     fi
}
```

- Vérification du commit des dépôts mercurial
  - Vérification des dépôts

```
function check_repo
{
    local REPO CWD
    REPO="$1"
    CWD="$PWD"
    cd "$REPO" && \
    status=`hg status -q`
    if [[ "$status" != "" ]]; then
        echo "2 DEPOT_$REPO test=1 CRITICAL - [le depot n'est pas commite]"
    else
        echo "0 DEPOT_$REPO test=0 OK - [le depot est commite]"
    fi
    cd "$CWD"
}
```

```
function check_repo_list
{
    local DIR HG_SUBDIR
    DIR=`grep "^/" $DEPOTFILE`
    for HG_SUBDIR in $DIR; do
        check_repo ${HG_SUBDIR%/.hg}
    done
}
```

- Résultat du lancement de l'agent Check_MK

```
<<<postfix_mailq>>>
Mail queue is empty
<<<apt>>>
6925
7.3
<<<logwatch>>>
[[[/var/log/messages]]]
[[[/var/log/auth.log]]]
[[[/var/log/syslog]]]
[[[/var/log/kern.log]]]
<<<local>>>
0 MONIT_apache2 uptime=1658040 OK - apache2 is monitored
0 MONIT_sogo uptime=520882 OK - sogo is monitored
0 MONIT_memcached uptime=1658039 OK - memcached is monitored
0 MONIT_perdition-pop3 uptime=2339333 OK - perdition-pop3 is monitored
0 MONIT_perdition-imap4 uptime=2339333 OK - perdition-imap4 is monitored
0 MONIT_postfix uptime=2339332 OK - postfix is monitored
0 MONIT_sshd uptime=2339333 OK - sshd is monitored
0 MONIT_system_sogo3.ac-lille.fr test=0 OK - system_sogo3.ac-lille.fr is monitored
0 LOCALHOST test=0 OK - 64 bytes from sogo3.ac-lille.fr (127.0.0.1): icmp_req=1 ttl=64 time=0.025 ms
0 DEPOT_/etc/apache2/ test=0 OK - [le depot est commite]
0 DEPOT_/home/sogo/ test=0 OK - [le depot est commite]
0 DEPOT_/home/sogo/groupe_collaboratif/daemon/ test=0 OK - [le depot est commite]
0 sshd-RootLogin test=0 OK - PermitRootLogin without-password
```

- Quelques commandes basiques:

✓ check_mk –I « host/hostgroup »
- Découverte des nouveaux services (pour un hôte existant)

✓ check_mk –II « host/hostgroup »
- Redécouverte complète des services (pour un nouvel hôte)

✓ check_mk –nvp « host/hostgroup »
- Vérification en temps réel de l'inventaire

✓ check_mk –R « host/hostgroup »
- Génération des fichiers pour Nagios + Validation de la configuration + Redémarrage de Nagios

Supervision: Utilisation de Check-MK

Capture d'Ecran (1)

- Interface Web de Check-MK: Vue principale

Supervision: Utilisation de Check-MK

Capture d'Ecran (2)

- Interface Web de Check-MK: Vue détaillée d'un hôte

filer.in.ac-lille.fr

State	Service	Icons	Status detail	Age	Checked	Perf-O-Meter
OK	Check_MK		OK - Agent version 1.2.5i1, execution time 15.0 sec	30 hrs	71 sec	15.0s
OK	CPU load		OK - 15min load 0.05 at 8 CPUs	2013-09-18 12:32:44	56 sec	0.0
OK	CPU utilization		OK - user: 0.6%, system: 0.3%, wait: 0.0%	2014-01-17 08:44:26	56 sec	0%
WARN	DellMaintenance		WARN - WARNING - le serveur n'est plus maintenu depuis -467 jours. Type : PowerEdge 2950 TAG : 2GTT63J	2014-01-17 08:44:26	56 sec	
OK	fs_/		OK - 75.7% used (5.82 of 7.7 GB), (levels at 90.00/95.00%), trend: +436.22kB / 24 hours	2014-01-26 12:09:21	56 sec	75.67%
OK	fs_/boot		OK - 38.8% used (0.07 of 0.2 GB), (levels at 90.00/95.00%), trend: -0.04B / 24 hours	2013-09-18 12:32:44	56 sec	38.78%
CRIT	fs_/mnt/DLL		CRIT - 97.2% used (239.22 of 246.1 GB), (levels at 90.00/95.00%), trend: +2.82GB / 24 hours	10 hrs	56 sec	97.21%
OK	Interface 2		OK - [eth0] (up) MAC: 00:15:17:48:c8:38, 1GBit/s, in: 52.65B/s, out: 77.92B/s	2014-01-17 08:44:26	56 sec	0.0% 0.0%
CRIT	Interface 3		CRIT - [eth1] (down) CRIT MAC: 00:15:17:48:c8:39, assuming 1GBit/s	53 min	56 sec	
OK	Interface 6		OK - [eth4] (up) MAC: 00:1d:09:05:c5:79, 1GBit/s, in: 5.06kB/s, out: 15.15kB/s	2014-01-17 08:44:26	56 sec	0.0% 0.0%
OK	Kernel Context Switches		OK - 346/s in last 60 secs	2014-01-17 08:44:26	56 sec	346.5/s
OK	Kernel Major Page Faults		OK - 0/s in last 60 secs	2014-01-17 08:44:26	56 sec	0.0/s
OK	Kernel Process Creations		OK - 7/s in last 60 secs	2014-01-17 08:44:26	56 sec	7.3/s
OK	LOCALHOST		OK - 64 bytes from localhost (127.0.0.1): icmp_seq=1 ttl=64 time=0.029 ms	2014-01-17 08:44:26	56 sec	
OK	LOG /var/log/messages		OK - no error messages	30 hrs	56 sec	
OK	Memory used		OK - 1.08 GB used (1.08 RAM + 0.00 SWAP + 0.01 Pagetables, this is 4.6% of 23.46 RAM), 0.0 mapped, 0.4 committed	2014-01-17 08:44:26	56 sec	4%
OK	Mount options of /		OK - mount options exactly as expected	2014-01-17 08:44:26	56 sec	
OK	Mount options of /boot		OK - mount options exactly as expected	2014-01-17 08:44:26	56 sec	
OK	Mount options of /mnt/DLL		OK - mount options exactly as expected	2014-01-17 08:44:26	56 sec	
CRIT	Multipath 36000d310002a47000000000000000034		CRIT - (dll-cplt) broken paths: 10:0:0:1(sdj)	51 min	56 sec	
OK	NTP Time		OK - sys.peer - stratum 3, offset -1.96 ms, jitter 0.48 ms, last reached 668 secs ago (synchronized on dns1.ac-lille.f)	2014-01-10 02:11:46	56 sec	-2.0 ms
OK	Number of threads		OK - 424 threads	2013-09-18 12:32:44	56 sec	424
OK	OM_Battery_probe_0		OK - [System Board CMOS Battery] is Good	2014-01-17 08:44:26	56 sec	
OK	OM_Chassis_fan_0		OK - [System Board FAN 1 RPM] reading: 7800 RPM	2014-01-17 08:44:26	56 sec	
OK	OM_Chassis_fan_1		OK - [System Board FAN 2 RPM] reading: 7875 RPM	2014-01-17 08:44:26	56 sec	
OK	OM_Chassis_fan_2		OK - [System Board FAN 3 RPM] reading: 7800 RPM	2014-01-17 08:44:26	56 sec	
OK	OM_Chassis_fan_3		OK - [System Board FAN 4 RPM] reading: 7875 RPM	2014-01-17 08:44:26	56 sec	
OK	OM_Connector_0		OK - [SAS Port RAID Mode] on controller 0 is Ready	2014-01-17 08:44:26	56 sec	
OK	OM_Connector_1		OK - [SAS Port RAID Mode] on controller 0 is Ready	2014-01-17 08:44:26	56 sec	
OK	OM_Controller_0		OK - [PERC 5/i Integrated] is Ready	2014-01-17 08:44:26	56 sec	
OK	OM_Enclosure_0:0:0		OK - [Backplane] on controller 0 is Ready	2014-01-17 08:44:26	56 sec	
OK	OM_Logical_Drive_/dev/sda		OK - [RAID-5, 836.63 GB] is Ready	2014-01-17 08:44:26	56 sec	

- Livestatus: Broker qui fournit l'état des hôtes et des services supervisés par Nagios
- Utilise une socket UNIX
  - ✓ Pas de stockage en base : Gain de performance
- Accès direct aux données sans écriture disque
- Plus de 50000 services récupérés < 2 secondes

- Console de supervision de Check-MK
- Permet d'agréger plusieurs systèmes de monitoring indépendants (Nagios / Shinken)
- Utilise Livestatus pour accéder aux données dans l'interface Web
- Interface intuitive et rapide

- Utilisé depuis 2 ans au Rectorat de LILLE

- Avant Check-MK :
  - ✓ **600** serveurs monitorés et environ **2000** services testés
  - ✓ Environ **20 minutes** pour que Nagios fasse les tests de supervision sur l'ensemble des serveurs

- Avec Check-MK:
  - ✓ **600** serveurs monitorés et près de **17000** services testés!
  - ✓ Environ **5 minutes** pour que Nagios fasse les tests de supervision sur l'ensemble des serveurs

- Plus de **8 fois plus** de services testés et pourtant les **ressources CPU** utilisées sur le serveur Nagios ont **baissées** significativement

- Lien du site officiel de Check-MK :

✓ http://mathias-kettner.de/check_mk.html

Des Questions ?