Gestión de Traps SNMP

Carlos Vicente
Servicios de Red
Universidad de Oregon

Contenido

- Qué son los *traps snmp*
- Herramientas:
  - snmptrapd
  - snmptt
  - Integración con Nagios

Gestión de Traps

- Los agentes snmp en dispositivos como routers, switches, printers, servidores, etc. pueden enviar alarmas (*traps)* cuando ocurren ciertos eventos:
  - Se “cae” una interfaz
  - Se estropea el ventilador de un router
  - La carga de procesos excede un límite
  - Se llena una partición de disco
  - Un UPS cambia de estado
- Es necesario un mecanismo inteligente para notificar al administrador sólo cuando interesa

Gestión de traps

- Una vez recogidos los traps, es útil hacer dos cosas:
  - Notificar inmediatamente al NOC de ciertos eventos
  - Generar reportes diarios (tipo *top-ten*)

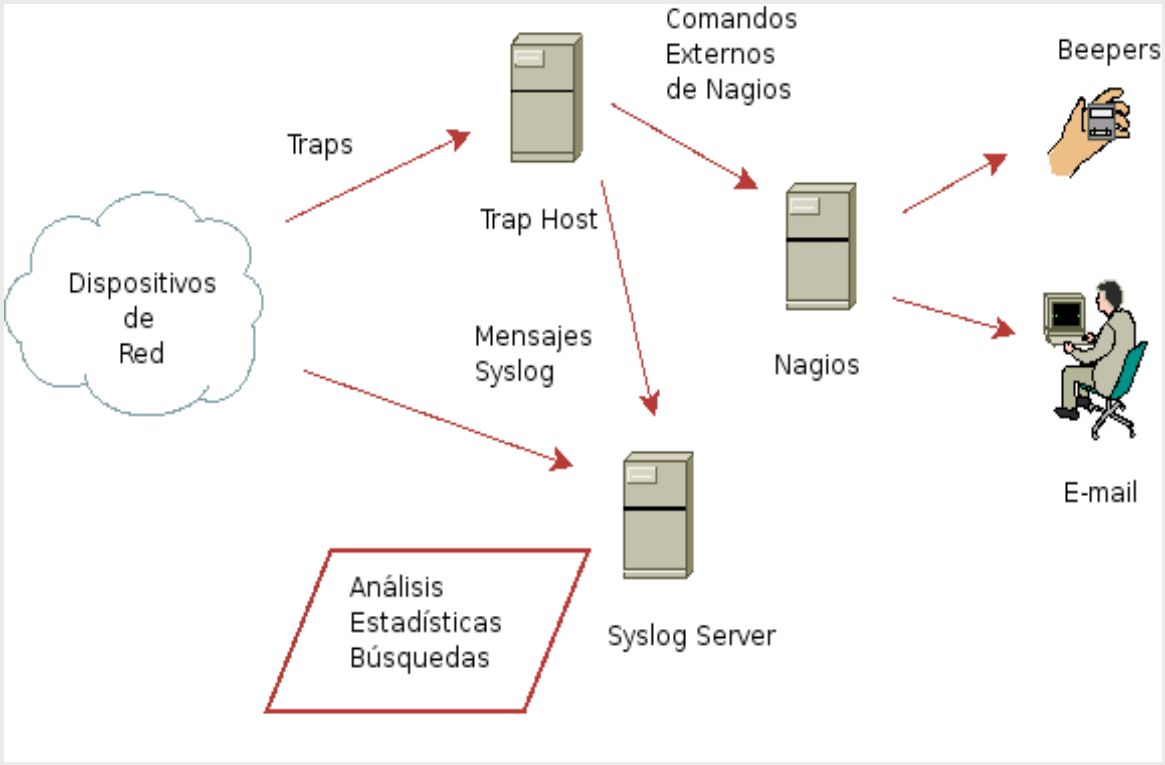
Traps y Syslog

- Es útil convertir los traps en mensajes Syslog y enviarlos al servidor syslog central
  - Un único sitio donde ir a buscar mensajes
  - Preferiblemente, con una base de datos

snmptrapd + snmptt + Nagios

- snmptrapd : *Daemon* incluído en paquete Net-SNMP
  - Simplemente recibe los traps via UDP y los pasa a algún gestionador
- snmptt = *SNMP Trap Translator*
  - Se integra con snmptrapd y permite manipular los traps con más flexibilidad
- Ciertos traps pueden ser capturados por snmptt con reglas de selección y enviados a otro software como Nagios
  - La integración con Nagios resuelve el problema de las notificaciones
    - Re-utilización de: grupos de contacto, períodos, mecanismo de mensajes a beepers, etc.

traps, syslog y Nagios



Configuración snmptrapd

/etc/snmp/snmptrapd.conf:

```
# Permitir las comunidades snmp siguientes:
authCommunity log,execute public
authCommunity log,execute walc

# Delegar toda la gestión a snmptt
traphandle default /usr/sbin/snmptthandler
```

Ejecución de snmptrapd

- Ver: *man snmptrapd*
- Opciones que nos interesan:

  -*t* : No enviar mensajes syslog (lo haremos con otra herramienta)

  -*On* : No traducir OIDs numéricos a nombres
- En Ubuntu (/etc/default/snmpd):
  - TRAPDOPTS='-t -On -p /var/run/snmptrapd.pid'

configuración snmptt

- /etc/snmp/snmptt.ini

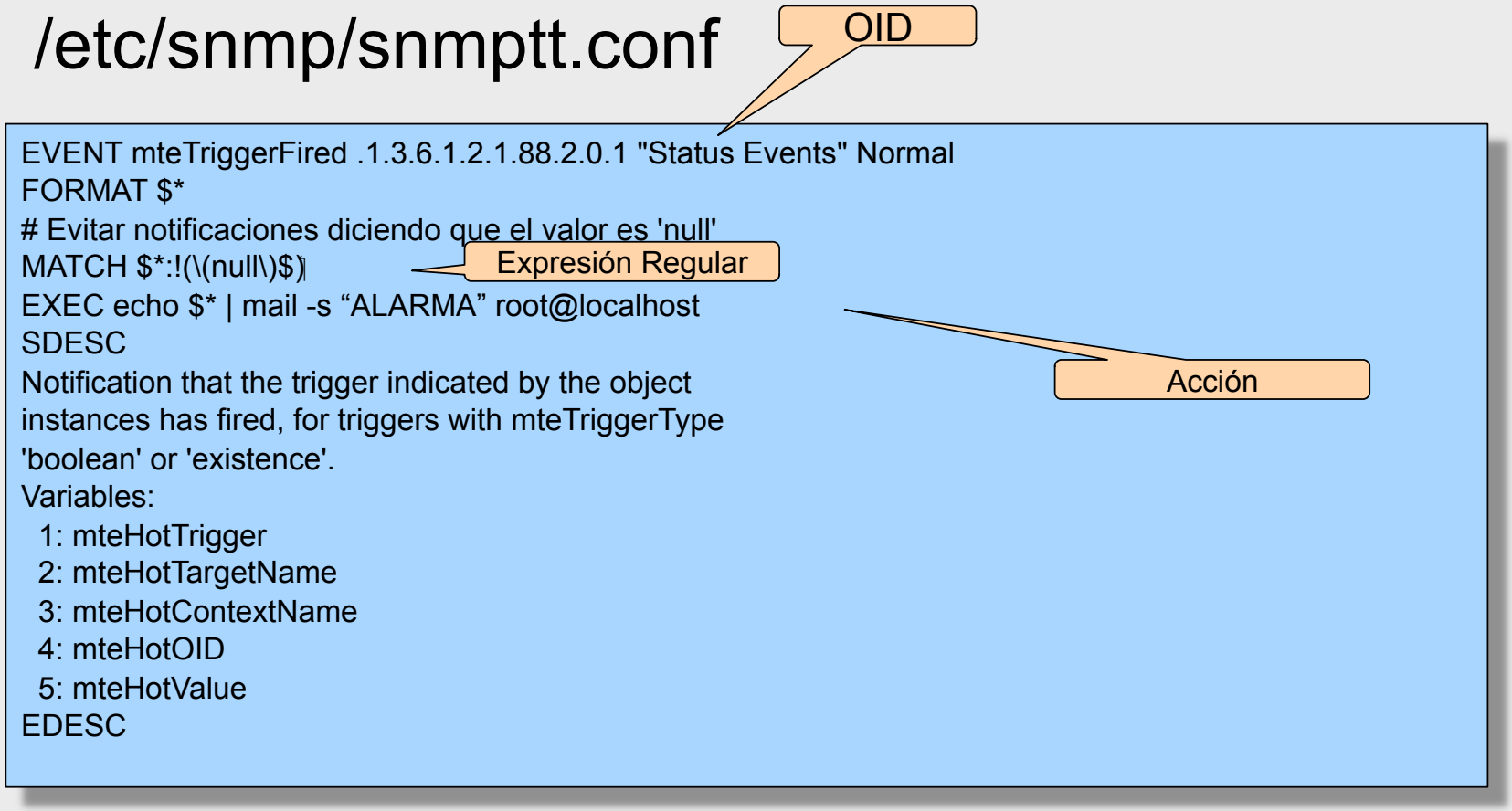
```
[General]
mode = daemon
dns_enable = 1
net_snmp_perl_enable = 1
translate_log_trap_oid = 1
translate_value_oids = 1
translate_enterprise_oid_format = 1
translate_trap_oid_format = 1
translate_varname_oid_format = 1
translate_integers = 1
keep_unlogged_traps = 1

[DaemonMode]
daemon_fork = 1
daemon_uid = snmptt
spool_directory = /var/spool/snmptt/
sleep = 1
use_trap_time = 1

[Logging]
stdout_enable = 0
syslog_enable = 1
syslog_level = info
syslog_facility = local6
[TrapFiles]
snmptt_conf_files = /etc/snmp/snmptt.conf
```

configuración snmptt

- /etc/snmp/snmptt.conf



snmpttconvertmib

- Utilitario para automatizar la creación de configuraciones snmptt a partir de un archivo MIB
- Ahorra mucho tiempo
- Requisito:
  - El directorio donde está la MIB debe estar incluido en la lista *mibdirs* del archivo /etc/snmp/snmp.conf

snmpttconvertmib

- Ejemplo:

snmpttconvertmib --in /usr/local/netdisco/mibs/cisco/CISCO-ERR-DISABLE-MIB.my --out /etc/snmp/snmptt.conf.cisco.errdisable

```
#
MIB: CISCO-ERR-DISABLE-MIB (file:/usr/local/netdisco/mibs/cisco/CISCO-ERR-DISABLE-MIB.my)
converted on Tue Oct 28 18:10:05 2008 using snmpttconvertmib v1.2
#
#
#
EVENT cErrDisableInterfaceEvent .1.3.6.1.4.1.9.9.548.0.1.1 "Status Events" Normal
FORMAT The cErrDisableInterfaceEvent is generated when an interface $*
SDESC
The cErrDisableInterfaceEvent is generated when an interface
or {interface, vlan} is error-disabled by the feature
specified in cErrDisableIfStatusCause.
Variables:
  1: cErrDisableIfStatusCause
EDESC
```

Snmpttconvertmib

- Luego de generar el archivo, hay que incluirlo en la lista:
  - En *snmptt.ini*:

```
[TrapFiles]
snmptt_conf_files = <<END
/etc/snmp/snmptt.conf
/etc/snmp/snmptt.conf.cisco.errdisable
END
```

Ejecución de snmptt

- /etc/init.d/snmptrapd start
  - Nota: En Ubuntu:
    - TRAPDRUN=yes
    - usar /etc/init.d/snmpd start
- /etc/init.d/snmptt start

Ejercicio

- Configurar snmptt para enviar traps cuando las interfaces “se caen”.
  - Usar *snmpttconvertmib* y la “IF-MIB”
  - Usar el comando mail para enviar la alarma a root@localhost
  - Comprobar enviando traps desde el enrutador
    - En Cisco, configurar así:

```
snmp-server enable traps snmp linkdown linkup
snmp-server trap link ietf
snmp-server host 192.168.0.10 version 2c public
```

Integración con Nagios

```
EVENT mteTriggerFired .1.3.6.1.2.1.88.2.0.1 "Status Events" Normal
FORMAT $*
EXEC /usr/local/nagios/libexec/eventhandlers/submit_check_result $r TRAP 2 "$*"
```

```
define service{
        name                            generic-trap
        active_checks_enabled           0
        service_description             TRAP
        is_volatile                     1
        check_command                   check-host-alive;
        max_check_attempts              1
        normal_check_interval           1
        retry_check_interval            1
        passive_checks_enabled          1
        check_period                    none
        notification_interval           31536000
        notification_period             24x7
        notification_options            c
        notifications_enabled           1
        flap_detection_enabled          0
        contact_groups                  nobody
        register                        0
}
```

Integración con Nagios

```
define service{
        name                            generic-trap
        active_checks_enabled           0
        service_description             TRAP
        is_volatile                     1
        check_command                   check-host-alive;
        max_check_attempts              1
        normal_check_interval           1
        retry_check_interval            1
        passive_checks_enabled          1
        check_period                    24x7
        notification_interval           31536000
        notification_period             24x7
        notification_options            c
        notifications_enabled           1
        flap_detection_enabled          0
        check_freshness                 1
        freshness_threshold             86400
        contact_groups                  nobody
        register                        0
}

define service{
        use                     generic-trap
        host_name               router1
        contact_groups          grupo-routers
}
```

Consideraciones de Seguridad

- Restringir el tráfico de traps en el servidor central
  - Sólo permitir que sus equipos envíen logs
  - Por ejemplo, usar iptables:

```
# iptables -A INPUT -s 192.168.1.0/24 -p udp --dport 162 -j ACCEPT
# iptables -A INPUT -s 0/0 -p udp --dport 162 -j REJECT
```

Referencias

- http://www.net-snmp.org
- http://www.snmptt.org