KdG Karel de Grote Hogeschool

Wat is Nagios?

- Open Source Network Monitoring Software
- De-facto standaard voor monitoring
  - 2002 ontstaan, heette toen “NetSaint”
  - Ondanks de populariteit:
    - Niet altijd even goed onderhouden
    - Laatste versies niet standaard beschikbaar in Linux

Alternatieven Nagios

- Shinken (Nagios compatible)
  - http://www.shinken-monitoring.org
- OpenNMS
- Icinga (Nagios compatible)
  - fork van Nagios (sinds 2010), Nagios Core developer voerde al twee jaar geen enkele bugfix meer uit

Nagios Configuratie

- **Configuratiebestanden zijn *Object based* en gebruiken *inheritance***
- **Objecten bij Nagios:**

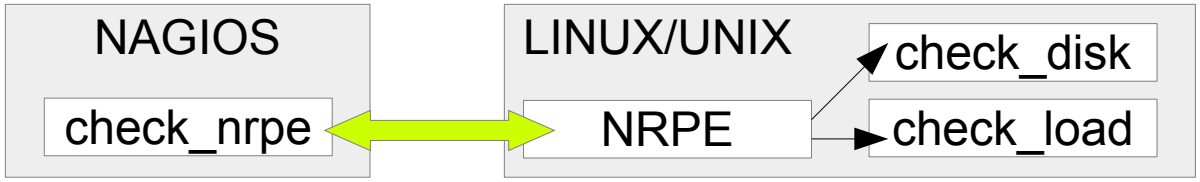
  - Host
  - Host Group
  - Service
  - Service Group
  - Time Periods
  - Contact
  - Contact Group
  - Extended Host Info
  - Extended Service Info
  - Command Definitions

Onderdelen

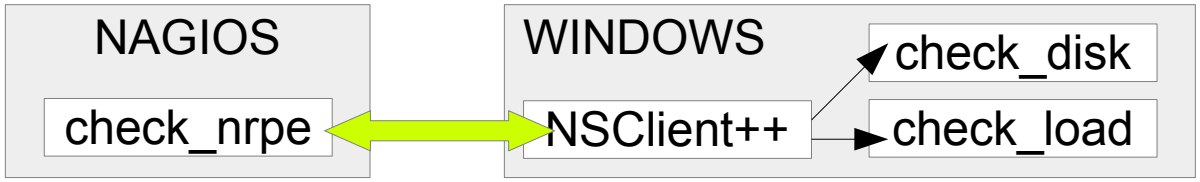
- Nagios Core (nagios4)
  - Server met webinterface/databank
- Nagios Plugins (nagios-plugins)
  - Reeks check scripts voor services

Client

- **NRPE (nagios-nrpe)**
  - **Nagios Remote Plugin Executor**
  - **Remote checks uitvoeren op Linux hosts**

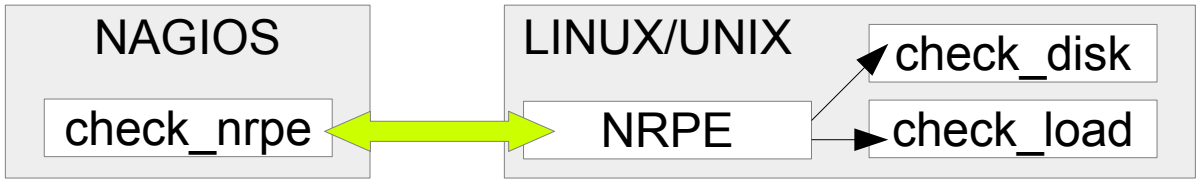


- **NSClient++ of nscp**
  - **Remote Checks uitvoeren op Windows hosts**



Deb pakketten

- **nagios-nrpe-client (draait op de "server")**
  - **installeert het programma** check_nrpe
- **nagios-nrpe-server (draait op de remote "client")**



NRPE test

- **Basis nrpe checks steken in het pakket monitoring-plugins-basic**

```
/usr/lib/nagios/plugins/check_nrpe -H localhost -c check_load

OK - load average: 0.22, 0.26, 0.14|
load1=0.220;15.000;30.000;0; load5=0.260;10.000;25.000;0;
load15=0.140;5.000;20.000;0;



/usr/lib/nagios/plugins/check_nrpe -H localhost -c check_users

USERS OK - 2 users currently logged in |users=2;5;10;0
```

Check script

- Binary of script in eender welke taal. Moet wel een exit code kunnen meegeven
  - bash, perl, python, c, ...
- De exit code bepaalt de status van de service op nagios
  - 0 Alles OK
  - 1 Warning
  - 2 Critical
  - 3 Unknown

Active/Passive checks

- Active Check
  - Server vraagt de client om een check uit te voeren en het resultaat terug te sturen
- Passive Check
  - Client kiest zelf wanneer hij/zij informatie naar de server doorstuurt
    - Services hebben dikwijls zelf al een monitoring systeem
    - Geen nieuws is goed nieuws
  - Client stuurt door naar een named pipe van Nagios

hosts

```
define host{
        host_name                       my-linux
        alias                           my-linux.kdg.be
        address                         10.172.14.2
        max_check_attempts              5
        check_interval                  5
        retry_interval                  1
        check_period                    24x7
        notification_interval           120
        notification_period             24x7
        notification_options            d,r
        contact_groups                  unix-admins
        register                        1
        }
```

Services

```
define service{
     name                                ping-service
     service_description                 PING
     is_volatile                         0
     check_period                        24x7
     max_check_attempts                  4
     normal_check_interval               5
     retry_check_interval                1
     contact_groups                      unix-admins
     notification_options                w,u,c,r
     notification_interval               960
     notification_period                 24x7
     check_command    check_ping!100.0,20%!
  500.0,60%
     hosts                               my-linux
     register                            1
     }
```

Command

- **Commands roepen een check script op**

```
define command{
  command_name    check-host-alive
  command_line    $USER1$/check_ping -H
                  $HOSTADDRESS$ -w 99,99% -c 100,100% -p 1

        }
```

- **en de alerts (bv bericht met email)**

```
define command{
        command_name    notify-by-email
        command_line    /usr/bin/printf "%b" "***** Nagios
 *****\n\nNotification Type: $NOTIFICATIONTYPE$\n\
nService: $SERVICEDESC$\nHost: $HOSTALIAS$\nAddress:
$HOSTADDRESS$\nState: $SERVICESTATE$\n\nDate/Time:
$LONGDATETIME$\n\nAdditional Info:\n\n$SERVICEOUTPUT$" |
/bin/mail -s "** $NOTIFICATIONTYPE$ alert -
$HOSTALIAS$/$SERVICEDESC$ is $SERVICESTATE$ **"
$CONTACTEMAIL$
        }
```

Contacts

- **Contacts zijn de mensen die een notificatie moeten krijgen:**

```
define contact{
        contact_name                    arne
        alias                           Arne de Bakker
        service_notification_period     24x7
        host_notification_period        24x7
        service_notification_options    w,u,c,r
        host_notification_options       d,r
        service_notification_commands   notify-by-email
        host_notification_commands      host-notify-by-email
        email                           arme.debakker@kdg.be
        }
```

- **Contactgroups bundelen een aantal contacts:**

```
define contactgroup{
        contactgroup_name       unix-admins
        alias                   Unix Administrators
        members                 arne
        }
```

Time Periods

- **Deze definiëren wanneer alerts mogen komen**
  - **bv niet op zondag, niet 's nachts**

```
define timeperiod{
        timeperiod_name 24x7
        alias           24 Hours A Day, 7 Days A Week
        sunday          00:00-24:00
        monday          00:00-24:00
        tuesday         00:00-24:00
        wednesday       00:00-24:00
        thursday        00:00-24:00
        friday          00:00-24:00
        saturday        00:00-24:00
        }
```

Remote checks

- Nagios server roept check_nrpe op
  - nrpe daemon op de host draait een lokaal script
  - stuurt de output terug naar de server

- Nrpe.cfg (op remote host):

```
command[check_load]=/usr/lib/nagios/plugins/check_load -w
   15,10,5 -c 30,25,20
```

Nagios.cfg (op Master server):

```
define command{
        command_name    check_nrpe_load
        command_line    $USER1$/check_nrpe -H $HOSTADDRESS$ -c
                        check_load
        }
```

Host Groups, Service Groups

- **Samenbundelen verschillende computers en verschillende services**

```
define hostgroup{
        hostgroup_name  all-webservers
        alias           Alle Linux Web servers
        }
define servicegroup{
        servicegroup_name       basis-services
        alias                   DNS, DHCP, LDAP Services
        }
```

Templates

- **Een template maakt de definitie van een host eenvoudiger**

```
define host{
        name                    generic-unix-host
        use                     generic-host
        check_command           check-host-alive
        max_check_attempts      5
        check_period            24x7
        notification_interval   120
        notification_period     24x7
        notification_options    d,r
        contact_groups          unix-admins
        register                0
        }
```

- **De host definieer je dan als volgt:**

```
define host{
        use                     generic-unix-host
        host_name               my-linux
        alias                   my-linux.kdg.be
        address                 10.172.14.2
}
```

Services en logs

- Server
  - nagios
    - sudo nagios4 -v /etc/nagios4/nagios.cfg # Config check!
    - sudo systemctl restart nagios4
    - sudo systemctl status nagios4
    - sudo cat /var/log/nagios4/nagios.log
  - apache2
    - sudo systemctl restart apache2
    - sudo systemctl status apache2
    - cat /var/log/apache2/error.log

Services en logs (client)

- Client
  - nagios-nrpe-server
    - sudo systemctl restart nagios-nrpe-server
    - sudo systemctl status nagios-nrpe-server
    - cat /var/log/syslog

- Controleer poort tcp:5666 voor nrpe

Verder

- NSCA, is een script/daemon paar waarmee je passieve checks kan draaien en de resultaten naar een commandfile schrijven op de server
  - Samen met eventhandlers kan je hiermee een hierarchie van Nagios servers maken
- Services en hosts kunnen afhangen van andere servers en hosts
  - bv als switch down is, geen notificaties sturen voor de webservers er achter