

A dark blue vertical bar runs down the left side of the page. A blue arrow points to the right from the bar, containing the date.

7/06/2018

Linux Services

Practicum week 3

An abstract line drawing in the bottom left corner, consisting of several thin, curved lines that sweep upwards and to the right, resembling stylized grass or reeds.

Jop Bakker

Linux Services

Practicum week 3

Auteur: Jop Bakker

Klas: ITV2C

Studentnummer: 359423

Opleiding: HBO-ICT

Onderwijsinstelling: Hanzehogeschool Groningen

Vak: Linux Services (ITVB17ITO2)

Docent: Thies Keulen (KEHT)

Inleverdatum: donderdag 7 juni 2018

Contents

Contents	3
1 Regex.....	4
2 Monitoring.....	5
2.1 Nagios.....	5
2.2 Syslog-ng.....	8
3 Client systeem.....	9
3.1 Nagios client.....	9
3.2 Syslog-ng "cliënt"	11
Literatuurlijst	13

1 Regex

Om alles van shaw.com en shaw.net te krijgen maak ik gebruik van de volgende combinatie van karakters: `[a-z,A-Z,0-9]+@(shaw.com|shaw.net)`. Dit geeft vervolgens het volgende resultaat op de standaard `access_log`:

```
jbakker@ubul604-jba-monitor:~$ grep -E -o "[a-z,A-Z,0-9]+@(shaw.com|shaw.net)" access_log
ppwctwentynine@shaw.com
jbakker@ubul604-jba-monitor:~$
```

Voor testdoeleinde zijn er nog twee regels toegevoegd aan `access_log`

```
pd95f99f2.dip.t-dialin.net - - [12/Mar/2004:13:18:57 -0800] "GET /razor.html HTTP/1.1" 200 2869
d97082.upc-d.chello.nl - - [12/Mar/2004:13:25:45 -0800] "GET /SpamAssassin.html HTTP/1.1" 200 7368
test@shaw.net
pizza@show.net
```

Het commando geeft nu het volgende als output:

```
jbakker@ubul604-jba-monitor:~$ grep -E -o "[a-z,A-Z,0-9]+@(shaw.com|shaw.net)" access_log
ppwctwentynine@shaw.com
test@shaw.net
```

2 Monitoring

Voor deze installatie/configuratie zijn de volgende systemen gebruikt:

Ubu1604-jba-monitor: 10.0.0.11

Ubu1604-dev-jba-minion: 10.0.0.4

2.1 Nagios

Voor het correct installeren van nagios is gebruik gemaakt van de volgende guides:

"Nagios Core - Installing Nagios Core From Source" (2018)

"How to Install Nagios Server Monitoring on Ubuntu 16.04" (2016)

Vorbereidingen

Voor het installeren van Nagios moeten er verschillende packages geïnstalleerd zijn. Dit wordt gedaan door het volgende commando:

```
sudo apt-get install -y autoconf gcc libc6 make wget unzip apache2 php  
libapache2-mod-php7.0 libgd2-xpm-dev
```

Downloaden

Voor het downloaden en uitpakken van Nagios-4.3.4 worden de volgende twee regels gebruikt:

```
wget -O nagioscore.tar.gz  
https://github.com/NagiosEnterprises/nagioscore/archive/nagios-4.3.4.tar.gz  
  
tar xzf nagioscore.tar.gz
```

Installeren

Voor het installeren van Nagios wordt de volgende gebruiker gemaakt:

```
sudo useradd nagios  
  
sudo usermod -a -G nagios www-data
```

Daarna worden de volgende commando's gebruikt om Nagios te installeren:

```
sudo ./configure --with-httpd-conf=/etc/apache2/sites-enabled
sudo make all
sudo make install
sudo make install-init
sudo make install-commandmode
sudo make install-config

sudo update-rc.d Nagios defaults
```

Apache2 updates

Om te zorgen dat Apache ook werkt met Nagios worden de volgende commando's uitgevoerd:

```
sudo make install-webconf
sudo a2enmod rewrite
sudo a2enmod cgi
```

Firewall

Hoewel momenteel de firewall van de server uitstaat voegen we wel alvast een "allow" rol toe voor wanneer de firewall geactiveerd wordt:

```
sudo ufw allow Apache
```

Nagios web user

Om in de web-client van Nagios in te kunnen loggen registreren we met het volgende commando een wachtwoord:

```
sudo htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin
```

Nagios plugin

Om Nagios de services van de machines te laten registreren installeren we de volgende plugin op dezelfde manier als nagios zelf:

```
wget --no-check-certificate -O nagios-plugins.tar.gz
https://github.com/nagios-plugins/nagios-plugins/archive/release-
2.2.1.tar.gz

tar xzf nagios-plugins.tar.gz

cd /tmp/nagios-plugins-release-2.2.1/

sudo ./tools/setup

sudo ./configure

sudo make

sudo make install
```

Resultaat

Na dit allemaal geïnstalleerd is komt de localhost zichtbaar in de nagios webinterface

Nagios Current Network Status
Last Updated: Thu Jun 7 14:42:22 UTC 2018
Updated every 90 seconds
Nagios® Core™ 4.3.4 - www.nagios.org
Logged in as nagiosadmin

View History For all hosts
View Notifications For All Hosts
View Host Status Detail For All Hosts

Host Status Totals

Up	Down	Unreachable	Pending
2	0	0	0

All Problems All Types

All Problems	All Types
0	2

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
12	0	0	1	0

All Problems All Types

All Problems	All Types
1	13

Service Status Details For All Hosts

Host	Service	Status	Last Check	Duration	Attempt	Status Information
localhost	Current Load	OK	06-07-2018 14:37:59	0d 2h 34m 23s	1/4	OK - load average: 0.06, 0.02, 0.00
	Current Users	OK	06-07-2018 14:38:37	0d 2h 38m 45s	1/4	USERS OK - 1 users currently logged in
	HTTP	OK	06-07-2018 14:39:14	0d 2h 38m 8s	1/4	HTTP OK: HTTP/1.1 200 OK - 11595 bytes in 0.000 second response time
	PING	OK	06-07-2018 14:39:52	0d 2h 37m 30s	1/4	PING OK - Packet loss = 0%; RTA = 0.08 ms
	Root Partition	OK	06-07-2018 14:40:29	0d 2h 36m 53s	1/4	DISK OK - free space: / 27912 MB (93.98% inode=98%):
	SSH	OK	06-07-2018 14:41:07	0d 2h 36m 15s	1/4	SSH OK - OpenSSH_7.2p2 Ubuntu-4ubuntu2.4 (protocol 2.0)
	Swap Usage	CRITICAL	06-07-2018 14:41:44	0d 2h 40m 38s	4/4	SWAP CRITICAL - 0% free (0 MB out of 0 MB) - Swap is either disabled, not present, or of zero size.
	Total Processes	OK	06-07-2018 14:37:22	0d 2h 35m 0s	1/4	PROCS OK: 47 processes with STATE = RSZDT
ubuntu_host	Check SSH	OK	06-07-2018 14:41:06	0d 1h 17m 16s	1/2	SSH OK - OpenSSH_7.2p2 Ubuntu-4ubuntu2.4 (protocol 2.0)
	Check Users	OK	06-07-2018 14:41:42	0d 2h 28m 40s	1/2	USERS OK - 1 users currently logged in
	Local Disk	OK	06-07-2018 14:42:17	0d 2h 28m 5s	1/2	DISK OK - free space: / 27912 MB (93.98% inode=98%):
	PING	OK	06-07-2018 14:42:07	0d 2h 28m 15s	1/2	PING OK - Packet loss = 0%; RTA = 2.22 ms
	Total Process	OK	06-07-2018 14:41:51	0d 2h 28m 31s	1/2	PROCS OK: 46 processes with STATE = RSZDT

Results 1 - 13 of 13 Matching Services

2.2 Syslog-ng

Voor het centraliseren van logbestanden etc installeren we syslog-ng op de monitoring server.

Installatie

```
Sudo apt-get install syslog-ng
```

Configuratie

Om ervoor te zorgen dat de logging "server" op de juiste poort naar berichten van andere machines luistert en deze op de correcte manier op de correcte locatie op slaat wordt het config bestand gevuld met de volgende opties:

```
@version: 3.5
@include "scl.conf"
@include "`scl-root`/system/tty10.conf"
options {
    time-reap(30);
    mark-freq(10);
    keep-hostname(yes);
};
source s_local { system(); internal(); };
source s_network {
    syslog(transport(tcp) port(514));
};
destination d_local {
    file("/var/log/syslog-ng/messages_${HOST}"); };
destination d_logs {
    file(
        "/var/log/syslog-ng/log.txt"
        owner("root")
        group("root")
        perm(0777)
    ); };
log { source(s_local); source(s_network); destination(d_logs); };
```

Om ervoor te zorgen dat de binnenkomende logs ook opgeslagen worden maken we een nieuwe folder en een tekstbestand aan:

```
sudo mkdir /var/log/syslog-ng/
sudo touch /var/log/syslog-ng/log
```


3 Client systeem

3.1 Nagios client

Installatie

Op de "client" wordt Nagios geïnstalleerd doormiddel het volgende commando:

```
sudo apt-get install nagios-nrpe-server nagios-plugin
```

Na de installatie wordt in het config bestand van nrpe het serveradres toegevoegd:

```
# SERVER ADDRESS
# Address that nrpe should bind to in case there are more than one interface
# and you do not want nrpe to bind on all interfaces.
# NOTE: This option is ignored if NRPE is running under either inetd or xinetd

server_address=10.0.0.11
```

Client toevoegen op de server

Om de cliënt daadwerkelijk toe te voegen op de server en om services te controleren wordt op de server een config file voor de cliënt gemaakt: (Dit is een kleiner voorbeeld bestand)

```
define host {
    use                linux-server
    host_name          ubuntu_host
    alias              Ubuntu Host
    address            10.0.0.4
    register           1
}

define service {
    host_name          ubuntu_host
    service_description PING
    check_command       check_ping!100.0,20%!500.0,60%
    max_check_attempts 2
    check_interval      2
    retry_interval      2
    check_period        24x7
    check_freshness     1
    contact_groups      admins
    notification_interval 2
    notification_period 24x7
    notifications_enabled 1
    register            1
}
```

Controle

Om te controleren of de nieuwe cliënt (host) is toegevoegd draaien we het volgende commando:

```
/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg
```

Dat ons wanneer het goed gaat laat zien dat er 2 hosts zijn:"

```
jbakker@ubul604-jba-monitor:~$ sudo /usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg

Nagios Core 4.3.4
Copyright (c) 2009-present Nagios Core Development Team and Community Contributors
Copyright (c) 1999-2009 Ethan Galstad
Last Modified: 2017-08-24
License: GPL

Website: https://www.nagios.org
Reading configuration data...
  Read main config file okay...
  Read object config files okay...

Running pre-flight check on configuration data...

Checking objects...
  Checked 13 services.
  Checked 2 hosts.
  Checked 1 host groups.
  Checked 0 service groups.
  Checked 1 contacts.
  Checked 1 contact groups.
  Checked 24 commands.
  Checked 5 time periods.
  Checked 0 host escalations.
  Checked 0 service escalations.
Checking for circular paths...
  Checked 2 hosts
  Checked 0 service dependencies
  Checked 0 host dependencies
  Checked 5 timeperiods
Checking global event handlers...
Checking obsessive compulsive processor commands...
Checking misc settings...

Total Warnings: 0
Total Errors: 0

Things look okay - No serious problems were detected during the pre-flight check
```

3.2 Syslog-ng "cliënt"

Op de cliënt worden de volgende applicaties geïnstalleerd:

Mariadb

```
apt-get -y install mariadb-server mariadb-client
```

Apache Web Server

```
apt-get -y install apache2  
apt-get -y install phpMyAdmin
```

PHP

```
apt-get -y install php7.0 libapache2-mod-php7.0  
service apache2 restart
```

Syslog-ng

```
sudo apt-get install syslog-ng
```

Om syslog-ng nu de apache files te laten versturen passen we de syslog-ng.conf aan:


Gemaakt met hulp van:

"Easy way to send apache2 logs to syslog-ng" (2012)

"Logging to a Remote Host with Syslog-ng" (2017)

```
@version: 3.5  
@include "scl.conf"  
@include "`scl-root`/system/tty10.conf"  
source s_local { system(); internal(); };  
destination d_syslog_tcp {  
    syslog("10.0.0.11" transport("tcp") port(514)); };  
log { source(s_local); destination(d_syslog_tcp); };  
  
source s_apache2 {  
    file("/var/log/apache2/access.log" flags(no-parse));  
    file("/var/log/apache2/error_log" flags(no-parse));  
};  
  
destination loghost { tcp("10.0.0.11" port(514)); };  
log { source(s_apache2); destination(loghost); };
```

Na het herstarten van de syslog-ng server en cliënt zal de cliënt nu zijn apache access.log en error.log updates doorsturen naar de server die deze vervolgens in zijn log bestand zet.

 jbakker@ubu1604-jba-monitor: /var/log/syslog-ng

```
GNU nano 2.5.3                               File: log
[Thu Jun 07 12:24:16.352487 2018] [mpm_event:notice] [pid 10257:tid 140322139101056] AH00489: A$
[Thu Jun 07 12:24:16.352559 2018] [core:notice] [pid 10257:tid 140322139101056] AH00094: Comman$
[Thu Jun 07 12:25:39.113759 2018] [mpm_event:notice] [pid 10257:tid 140322139101056] AH00493: S$
AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using $
[Thu Jun 07 12:25:39.162744 2018] [mpm_event:notice] [pid 10257:tid 140322139101056] AH00489: A$
[Thu Jun 07 12:25:39.162754 2018] [core:notice] [pid 10257:tid 140322139101056] AH00094: Comman$
[Thu Jun 07 12:26:21.479806 2018] [mpm_event:notice] [pid 10257:tid 140322139101056] AH00491: c$
[Thu Jun 07 12:26:21.898188 2018] [mpm_prefork:notice] [pid 17685] AH00163: Apache/2.4.18 (Ubun$
[Thu Jun 07 12:26:21.898273 2018] [core:notice] [pid 17685] AH00094: Command line: '/usr/sbin/a$
[Thu Jun 07 12:26:25.765555 2018] [mpm_prefork:notice] [pid 17685] AH00169: caught SIGTERM, shu$
```

Literatuurlijst

Nagios Core - Installing Nagios Core From Source. (2018, 7 januari). Geraadpleegd op 7 mei 2018, van <https://support.nagios.com/kb/article/nagios-core-installing-nagios-core-from-source-96.html#Ubuntu>

Arul, M. (2016, 29 november). How to Install Nagios Server Monitoring on Ubuntu 16.04. Geraadpleegd van <https://www.howtoforge.com/tutorial/ubuntu-nagios/>

Easy way to send apache2 logs to syslog-ng. (2012, 18 mei). Geraadpleegd op 7 mei 2018, van <https://www.chrisnewland.com/easy-way-to-send-apache2-logs-to-syslog-ng-220>

Eck, R. (2017, 8 juni). Logging to a Remote Host with Syslog-ng. Geraadpleegd van <http://www.monitis.com/blog/logging-to-a-remote-host-with-syslog-ng>