

NAGIOS

Nagios คือหนึ่งในโปรแกรมหลักของ network management และ monitoring (Nagios, Cacti, Spokeping) Nagios คือโปรแกรมฟรีที่สามารถใช้สำหรับ Infrastructure monitoring ซึ่งโปรแกรมจะ monitor servers, switches, applications และ services โดยจะมีการแจ้งเตือนไปที่ System Administrator เมื่อมีบางอย่างผิดปกติและจะแจ้งเตือนกลับอีกครั้งเมื่อปัญหาได้รับการแก้ไขแล้ว

ในเอกสารนี้จะเป็นการใช้ 2 ระบบดังนี้

Nagios server:

Operating system : CentOS 6.5 32bits(Fresh)

IP Address : 10.0.0.2/24

Nagios client:

Operating System : CentOS 6.5 32bits(Fresh)

IP Address : 10.0.0.1/24

Windows client:

Operating System : Windows 7

IP Address : 10.0.0.3/24

ขั้นตอนการดำเนินงาน

1. เพิ่มและเปิดใช้ EPEL repository
2. ติดตั้ง Packages บน Monitoring Server
3. ติดตั้งและแก้ไข Nagios Server
4. เพิ่ม Host เพื่อทำการ Monitoring
5. เพิ่ม Host - Window Client
6. การ Monitoring

ขั้นตอนที่ 1 เพิ่มและเปิดใช้ EPEL repository

หลังจากที่ Nagios แสดงใน CentOS official ให้ทำการเพิ่ม EPEL repository เพื่อติดตั้ง Nagios และไปที่ Terminal แล้ว login ด้วย root

```
#wget http://dl.fedoraproject.org/pub/epel/6/x86_64/epel-release-6-8.noarch.rpm
```

```
#rpm -Uvh epel-release-6*.rpm
```

```
[root@slave ~]# wget http://dl.fedoraproject.org/pub/epel/6/x86_64/epel-release-6-8.noarch.rpm
--2014-09-29 10:45:09-- http://dl.fedoraproject.org/pub/epel/6/x86_64/epel-release-6-8.noarch.rpm
Resolving dl.fedoraproject.org... 209.132.181.25, 209.132.181.26, 209.132.181.27, ...
Connecting to dl.fedoraproject.org|209.132.181.25|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 14540 (14K) [application/x-rpm]
Saving to: "epel-release-6-8.noarch.rpm"

100%[=====>] 14,540      56.8K/s   in 0.3s

2014-09-29 10:45:13 (56.8 KB/s) - "epel-release-6-8.noarch.rpm" saved [14540/14540]

[root@slave ~]# sudo rpm -Uvh epel-release-6*.rpm
warning: epel-release-6-8.noarch.rpm: Header V3 RSA/SHA256 Signature, key ID 0608b895: NOKEY
Preparing...
 1:epel-release
[root@slave ~]# sudo rpm -Uvh epel-release-6*.rpm
```

ขั้นตอนที่ 2 ติดตั้ง Package บน Monitoring Server

ใช้คำสั่ง `#yum install gd gd-devel gcc glibc glibc-commo` หลังจาก run แล้วพิมพ์ `y` เพื่อยืนยันการติดตั้ง

```
root@slave:/opt/observium
File Edit View Search Terminal Help
(1/16): cloop-ppl-0.15.7-1.2.el6.i686.rpm | 93 kB 00:04
http://centos.ustc.edu.cn/centos/6.5/os/i386/Packages/cpp-4.4.7-4.el6.i686.rpm: [Errno 12] Timeout on http://centos.ustc.edu.cn/centos/6.5/os/i386/Packages/cpp-4.4.7-4.el6.i686.rpm: (28, 'Operation too slow. Less than 1 bytes/sec transferred the last 30 seconds')
Trying other mirror.
http://mirror.bit.edu.cn/centos/6.5/os/i386/Packages/cpp-4.4.7-4.el6.i686.rpm: [Errno 12] Timeout on http://mirror.bit.edu.cn/centos/6.5/os/i386/Packages/cpp-4.4.7-4.el6.i686.rpm: (28, 'Operation too slow. Less than 1 bytes/sec transferred the last 30 seconds')
Trying other mirror.
(2/16): cpp-4.4.7-4.el6.i686.rpm | 3.4 MB 00:04
(3/16): fontconfig-devel-2.8.0-3.el6.i686.rpm | 209 kB 00:02
(4/16): freetype-devel-2.3.11-14.el6_3.1.i686.rpm | 364 kB 00:03
(5/16): gcc-4.4.7-4.el6.i686.rpm | 8.2 MB 00:57
(6/16): gd-devel-2.0.35-11.el6.i686.rpm | 78 kB 00:01
(7/16): libX11-devel-1.5.0-4.el6.i686.rpm | 1.0 MB 00:11
(8/16): libXau-devel-1.0.6-4.el6.i686.rpm | 14 kB 00:00
(9/16): libXpm-devel-3.5.10-2.el6.i686.rpm | 33 kB 00:00
(10/16): libjpeg-turbo-devel-1.2.1-3.el6_5.i686.rpm | 96 kB 00:02
(11/16): libpng-devel-1.2.49-1.el6_2.i686.rpm | 112 kB 00:01
(12/16): libxcb-devel-1.8.1-1.el6.i686.rpm | 174 kB 00:02
(13/16): mpfr-2.4.1-6.el6.i686.rpm | 153 kB 00:01
(14/16): ppl-0.10.2 (91%) 23% [== ] 45 kB/s | 301 kB 00:21 ETA
```

ขั้นตอนที่ 3 ติดตั้งและแก้ไข Nagios

3.1 ติดตั้ง plug-ins และ nagios agents(nrpe-agent) ด้วยคำสั่ง `# yum install nagios*` พิมพ์ `y` ยืนยันการติดตั้ง

```

root@slave:/opt/observium
File Edit View Search Terminal Help
(80/119): nagios-plugins-rhev-1.0.0-2.el6.noarch.rp | 13 kB 00:00
(81/119): nagios-plugins-rpc-1.4.16-10.el6.i686.rpm | 16 kB 00:00
(82/119): nagios-plugins-sensors-1.4.16-10.el6.i686 | 14 kB 00:00
(83/119): nagios-plugins-smtp-1.4.16-10.el6.i686.rp | 37 kB 00:00
(84/119): nagios-plugins-snmp-1.4.16-10.el6.i686.rp | 37 kB 00:00
(85/119): nagios-plugins-ssh-1.4.16-10.el6.i686.rpm | 30 kB 00:00
(86/119): nagios-plugins-swap-1.4.16-10.el6.i686.rp | 31 kB 00:00
(87/119): nagios-plugins-tcp-1.4.16-10.el6.i686.rpm | 37 kB 00:00
(88/119): nagios-plugins-time-1.4.16-10.el6.i686.rp | 30 kB 00:00
(89/119): nagios-plugins-ups-1.4.16-10.el6.i686.rpm | 33 kB 00:00
(90/119): nagios-plugins-users-1.4.16-10.el6.i686.r | 28 kB 00:00
(91/119): nagios-plugins-wave-1.4.16-10.el6.i686.rp | 14 kB 00:00
(92/119): nrpe-2.15-2.el6.i686.rpm | 224 kB 00:00
(93/119): ntp-4.2.6p5-1.el6.centos.i686.rpm | 586 kB 02:09
(94/119): ntpdate-4.2.6p5-1.el6.centos.i686.rpm | 74 kB 00:05
(95/119): perl-Class-Accessor-0.31-6.1.el6.noarch.r | 26 kB 00:04
(96/119): perl-Config-Tiny-2.12-7.1.el6.noarch.rpm | 23 kB 00:00
(97/119): perl-Crypt-DES-2.05-9.el6.i686.rpm | 19 kB 00:00
(98/119): perl-Digest-HMAC-1.01-22.el6.noarch.rpm | 22 kB 00:05
(99/119): perl-Digest-SHA1-2.12-2.el6.i686.rpm | 49 kB 00:03
(100/119): perl-Math-Calc-Units-1.07-6.el6.noarch.r | 41 kB 00:00
(101/119): perl-Nagios-Plugin-0.35-1.el6.noarch.rpm | 61 kB 00:00
(102/119): perl-Net-SNMP-5.2.0-4.el6.noarch.rpm | 100 kB 00:00
[103/119]: perl-Par (30%) 51% [===== ] 93 B/s | 38 kB 06:38 ETA

```

```

root@slave:/opt/observium
File Edit View Search Terminal Help
perl-Readonly          noarch 1.03-11.el6          base 22 k
perl-Readonly-XS       i686  1.05-3.el6          base 14 k
perl-Sort-Versions     noarch 1.5-12.el6          epel 12 k
perl-Time-HiRes        i686  4:1.9721-136.el6   base 48 k
pnp4nagios            i686  0.6.22-2.el6       epel 2.4 M
postgresql-libs       i686  8.4.20-1.el6_5     updates 205 k
python-dateutil        noarch 1.4.1-6.el6         base 84 k
python-ldap            i686  2.3.10-1.el6       base 124 k
python-paramiko        noarch 1.7.5-2.1.el6      base 728 k
qstat                  i686  2.11-9.20080912svn311.el6 epel 158 k
radiusclient-ng        i686  0.5.6-5.el6        epel 42 k
rpcbind                i686  0.2.0-11.el6       base 51 k
rrdtool-perl           i686  1.3.8-6.el6        base 36 k
samba-client           i686  3.6.9-169.el6_5    updates 11 M
voms                   i686  2.0.11-7.el6       epel 148 k
yum-plugin-security    noarch 1.1.30-17.el6_5    updates 38 k

Transaction Summary
=====
Install      119 Package(s)

Total download size: 21 M
Installed size: 72 M
Is this ok [y/N]: y

```


3.3 ตั้งรหัสผ่านของ Nagiosadmin

* ใช้คำสั่ง `# htpasswd /etc/nagios/passwd nagiosadmin`

```

root@slave:~
File Edit View Search Terminal Help
[root@slave ~]# htpasswd /etc/nagios/passwd nagiosadmin
New password:
Re-type new password:
Updating password for user nagiosadmin
[root@slave ~]#

```

* เริ่ม nagios และบริการ httpd แล้วปล่อยให้ตัวโปรแกรมเริ่มอัตโนมัติบนทุกๆ boot

```
# service nagios start
```

```
# service httpd start
```

```
# chkconfig nagios on
```

```
# chkconfig httpd on
```

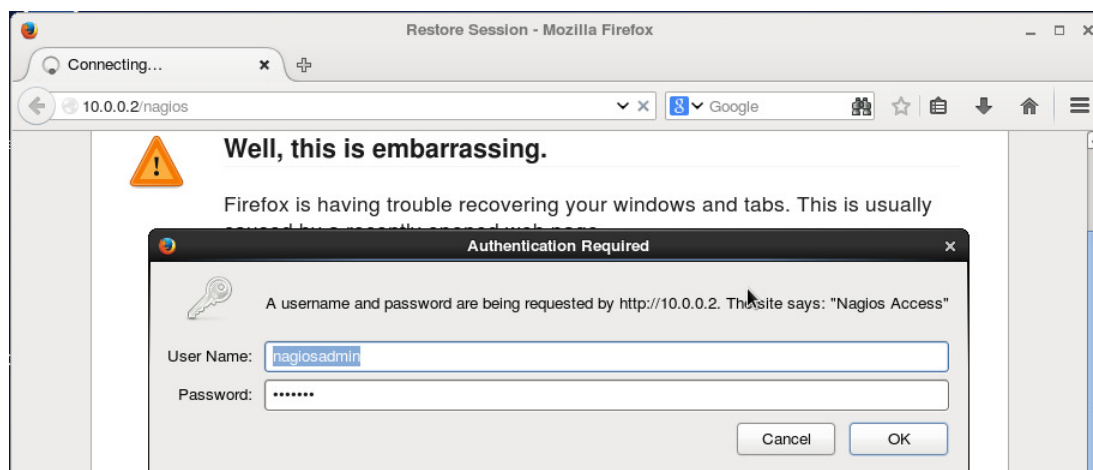
```

root@slave:~
File Edit View Search Terminal Help
[root@slave ~]# service nagios start
Starting nagios: done.
[root@slave ~]# service httpd start
Starting httpd:
[root@slave ~]# chkconfig nagios on
[root@slave ~]# chkconfig httpd on
[root@slave ~]#

```

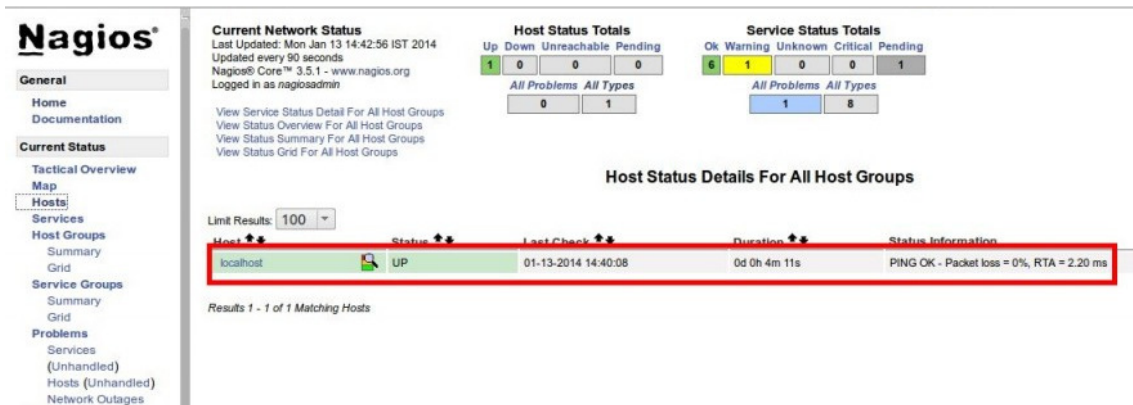
3.4 เข้าใช้งาน Nagios admin console

* เปิด nagios administrator console ด้วย URL `http://10.0.0.2/nagios` ใส่ username: nagiosadmin และรหัสผ่านที่เราได้สร้างไว้ก่อนหน้านี้

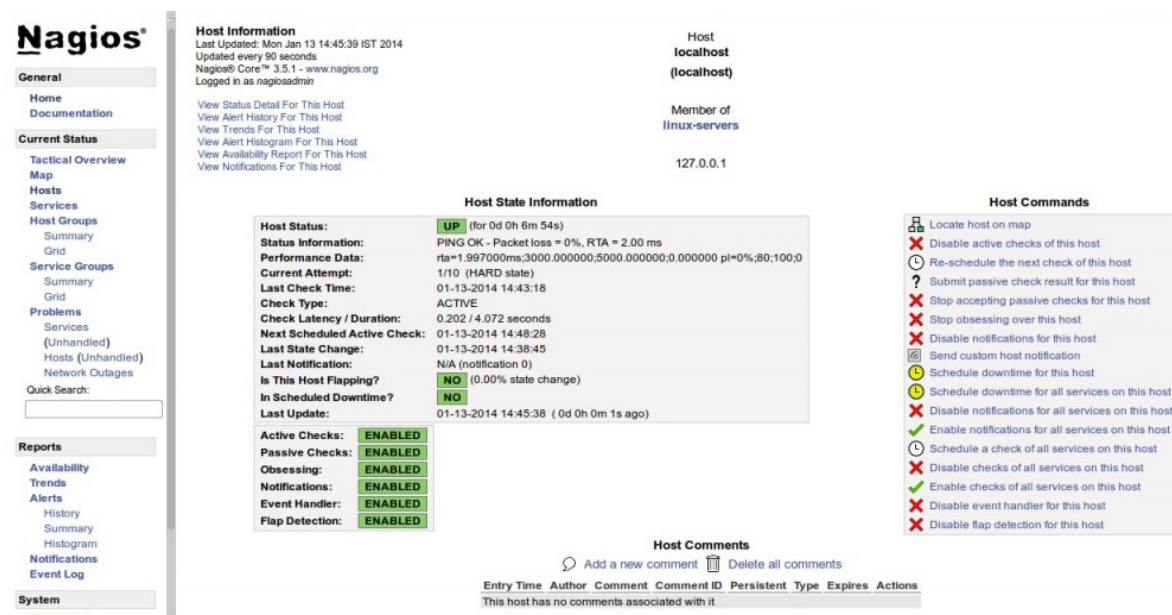




* เลือกเมนู “Hosts” ทางแถบด้านซ้าย จะเห็น Host ทั้งหมดที่เราต้องการตรวจสอบด้วย Nagios server ซึ่งในตอนนี้จะแสดงเพียง nagios server (localhost)



* เลือก localhost เพื่อแสดงข้อมูลทั้งหมด



ขั้นตอนที่ 4 เพิ่ม Host เพื่อ Monitoring

4.1 เพิ่ม EPEL repository ที่เครื่อง client เพื่อติดตั้ง nrpe package ก่อนทำการติดตั้ง nrpe และ nagios-plugins

ติดตั้ง “nrpe” และ “nagios-plugins” ที่ client ด้วยคำสั่ง

```
# wget http://dl.fedoraproject.org/pub/epel/6/x86_64/epel-release-6-8.noarch.rpm
# rpm -Uvh epel-release-6*.rpm
# yum install nrpe nagios-plugins-all openssl
```

```
[root@slave ~]# wget http://dl.fedoraproject.org/pub/epel/6/x86_64/epel-release-6-8.noarch.rpm
--2014-09-29 10:45:09-- http://dl.fedoraproject.org/pub/epel/6/x86_64/epel-release-6-8.noarch.rpm
Resolving dl.fedoraproject.org... 209.132.181.25, 209.132.181.26, 209.132.181.27, ...
Connecting to dl.fedoraproject.org|209.132.181.25|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 14540 (14K) [application/x-rpm]
Saving to: "epel-release-6-8.noarch.rpm"

100%[=====>] 14,540      56.8K/s  in 0.3s

2014-09-29 10:45:13 (56.8 KB/s) - "epel-release-6-8.noarch.rpm" saved [14540/14540]

[root@slave ~]# sudo rpm -Uvh epel-release-6*.rpm
warning: epel-release-6-8.noarch.rpm: Header V3 RSA/SHA256 Signature, key ID 0608b895: NOKEY
Preparing...
 1:epel-release
[root@slave ~]# sudo rpm -Uvh epel-release-6*.rpm
```

4.2 Configure Monitoring targets

* แก้ไขที่ไฟล์ `/etc/nagios/nrpe.cfg` โดยใช้คำสั่ง `# vi /etc/nagios/nrpe.cfg`

* เพิ่ม ip address ของ Nagios server ด้วย

Line 81 - Add the Nagios server IP

allowed_hosts=127.0.0.1 10.0.0.2

```
hadoop@master:~
File Edit View Search Terminal Help
# (i.e. 192.168.1.0/24) are also supported. Hostname wildcards are not currently
# supported.
#
# Note: The daemon only does rudimentary checking of the client's IP
# address. I would highly recommend adding entries in your /etc/hosts.allow
# file to allow only the specified host to connect to the port
# you are running this daemon on.
#
# NOTE: This option is ignored if NRPE is running under either inetd or xinetd
allowed_hosts=127.0.0.1 10.0.0.2
#
# COMMAND ARGUMENT PROCESSING
# This option determines whether or not the NRPE daemon will allow clients
# to specify arguments to commands that are executed. This option only works
# if the daemon was configured with the --enable-command-args configure script
# option.
#
# *** ENABLING THIS OPTION IS A SECURITY RISK! ***
# Read the SECURITY file for information on some of the security implications
```

4.3 เริ่ม nrpe service:

```
# service nrpe start
# chkconfig nrpe on
```

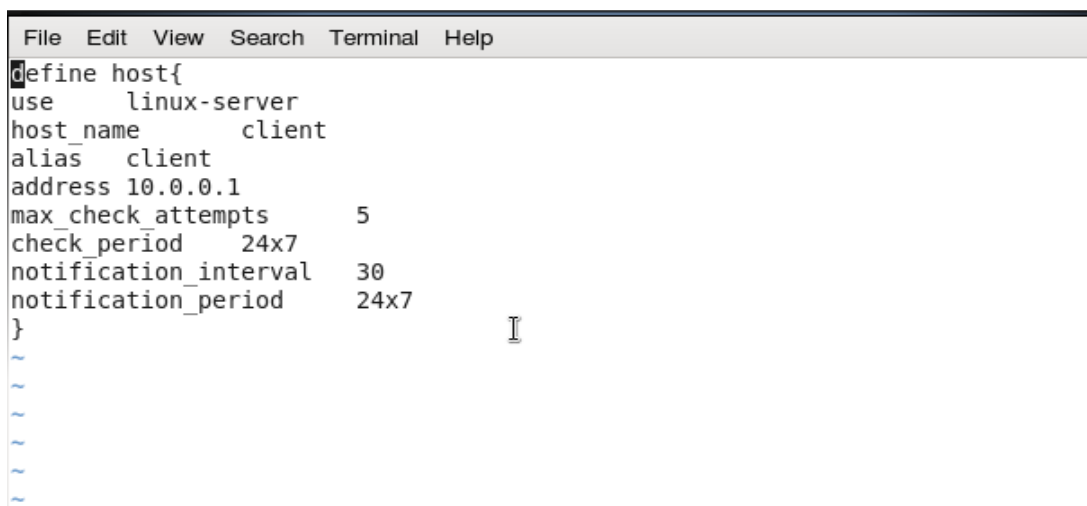
4.4 กลับไปที่ Nagios server เพื่อเพิ่ม client ผ่าน nagios server แก้ไขที่ไฟล์ `/etc/nagios/nrpe.cfg` โดยใช้คำสั่ง `# vi /etc/nagios/nrpe.cfg` และ uncomment ตามบรรทัดด้านล่าง

```
## Line 52 - Uncomment ##
cfg_dir=/etc/nagios/servers
```

4.5 สร้าง directory ที่เรียกว่า “servers” ภายใต้ “/etc/nagios/” ด้วยคำสั่ง `# mkdir /etc/nagios/servers`

4.6 สร้าง config file เพื่อ monitor Client ด้วยคำสั่ง `# vi /etc/nagios/servers/clients.cfg`

```
define host{
use          linux-server
host_name    client
alias        client
address      10.0.0.1
max_check_attempts    5
check_period    24x7
notification_interval    30
notification_period    24x7
}
```



```
File Edit View Search Terminal Help
define host{
use          linux-server
host_name    client
alias        client
address      10.0.0.1
max_check_attempts    5
check_period    24x7
notification_interval    30
notification_period    24x7
}
```


4.7 ทำการเพิ่ม Service เพื่อเก็บข้อมูล Monitoring ต่างๆ

```
#services
```

```
define service {
    use                generic-service
    host_name          client
    service_description SSH
    check_command      check_ssh
    notifications_enabled 0
}

define service{
    use                generic-service
    host_name          client
    service_description PING
    check_command      check_ping!100.0,20%!500.0,60%
}

define service{
    use                generic-service
    host_name          client
    service_description Root Partition
    check_command      check_local_disk!20%!10%!/
}

define service{
    use                generic-service
    host_name          client
    service_description Current Users
    check_command      check_local_users!20!50
}

define service{
    use                generic-service
    host_name          client
    service_description Total Processes
    check_command      check_local_procs!250!400!RSZDT
}

define service{
    use                generic-service
    host_name          client
```

```

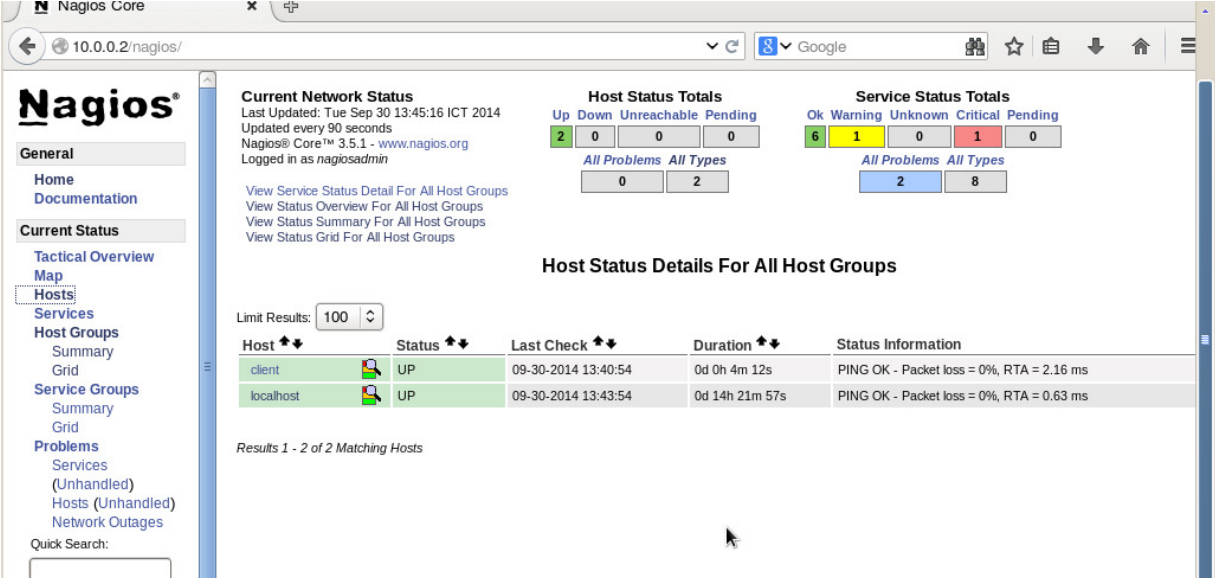
service_description      Current Load
check_command            check_local_load!5.0,4.0,3.0!10.0,6.0,4.0
}

define service{
    use                    generic-service
    host_name              client
    service_description    Swap Usage
    check_command          check_local_swap!20!10
}

define service{
    use                    generic-service
    host_name              client
    service_description    HTTP
    check_command          check_http
    notifications_enabled  0
}

```

4.8 ทำการ restart Nagios service ด้วยคำสั่ง `# service nagios restart` เมื่อเสร็จแล้วให้ทำการเปิด Nagios admin console ที่ Browser และเลือกเมนู “Hosts” ที่แถบด้านซ้าย จะเห็นว่ามี client เพิ่มมาที่ Host ดังรูป จากนั้นจะสามารถคลิกที่ Client เพื่อติดตามตรวจสอบหากมีสิ่งผิดปกติเกิดขึ้นได้



The screenshot shows the Nagios Core web interface. The browser address bar displays `10.0.0.2/nagios/`. The page title is "Nagios Core". The main content area is divided into several sections:

- Current Network Status:** Last Updated: Tue Sep 30 13:45:16 ICT 2014. Updated every 90 seconds. Nagios® Core™ 3.5.1 - www.nagios.org. Logged in as `nagiosadmin`.
- Host Status Totals:** A table showing counts for Up (2), Down (0), Unreachable (0), and Pending (0).
- Service Status Totals:** A table showing counts for Ok (6), Warning (1), Unknown (0), Critical (1), and Pending (0).
- Host Status Details For All Host Groups:** A table with columns: Host, Status, Last Check, Duration, and Status Information. It lists two hosts:

Host	Status	Last Check	Duration	Status Information
client	UP	09-30-2014 13:40:54	0d 0h 4m 12s	PING OK - Packet loss = 0%, RTA = 2.16 ms
localhost	UP	09-30-2014 13:43:54	0d 14h 21m 57s	PING OK - Packet loss = 0%, RTA = 0.63 ms

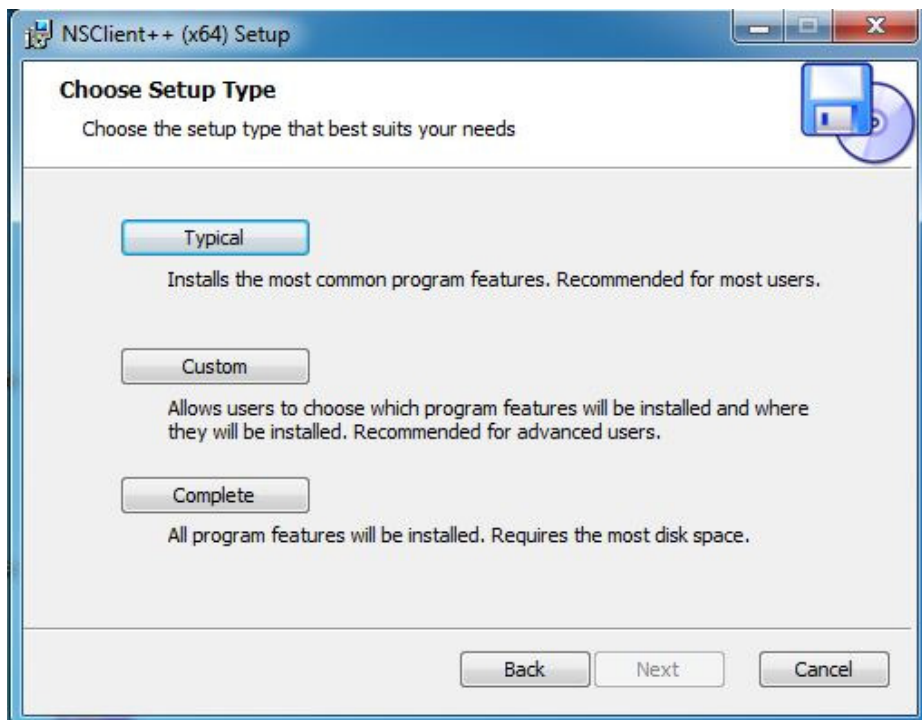
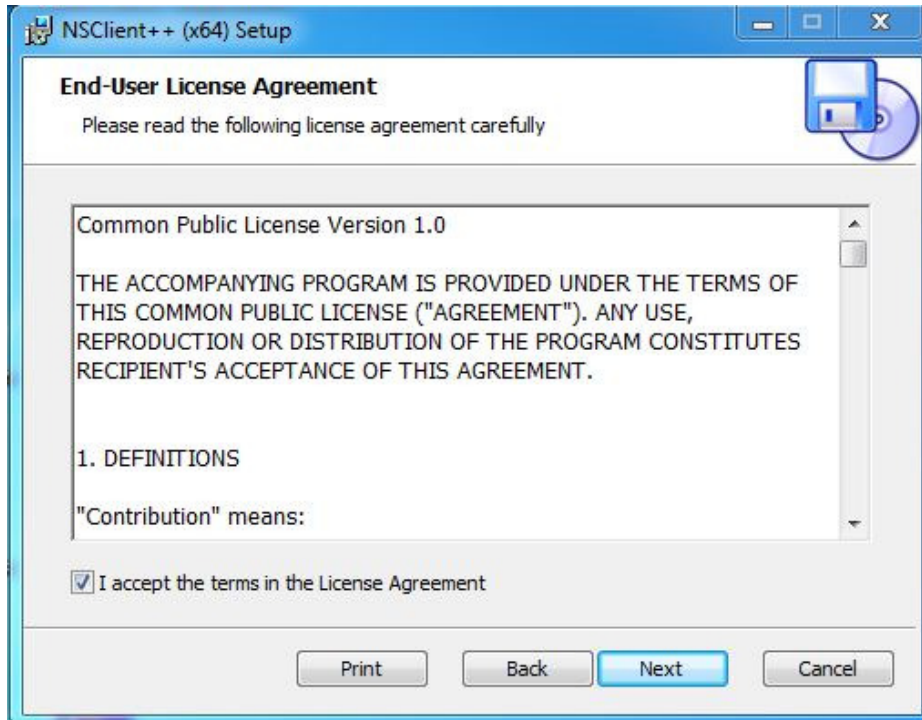
(สามารถศึกษาข้อมูลเพิ่มเติมได้ที่ <http://www.nagios.com/>)

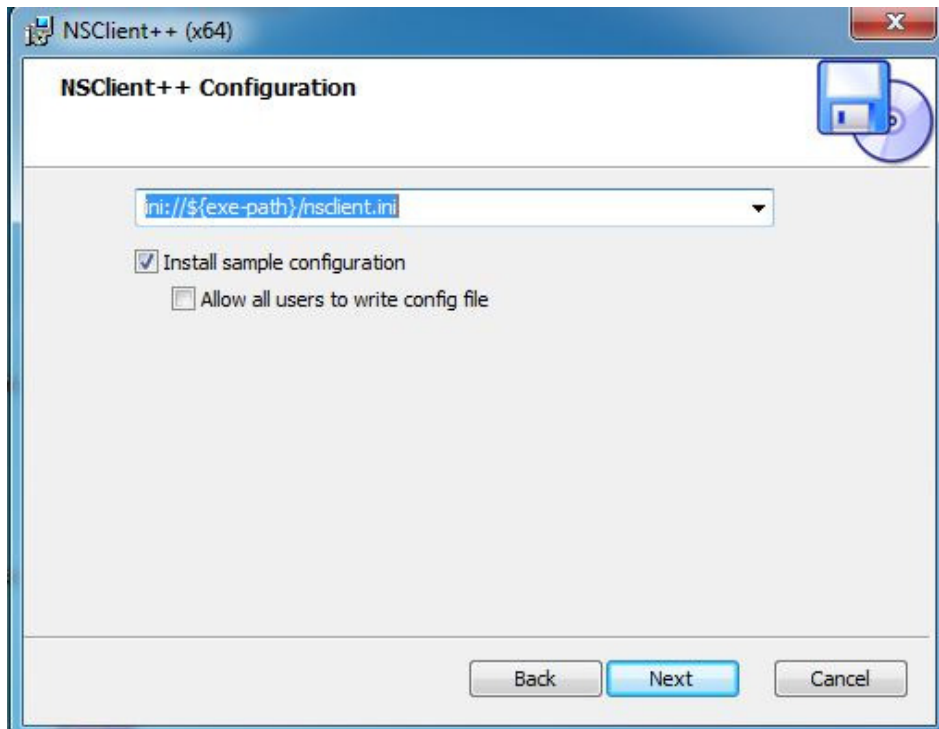
ขั้นตอนที่ 5 เพิ่ม Host - Windows Client

- ให้ติดตั้ง NSClient++ NagiosClient ใน Windows client
- Configure Nagios Server

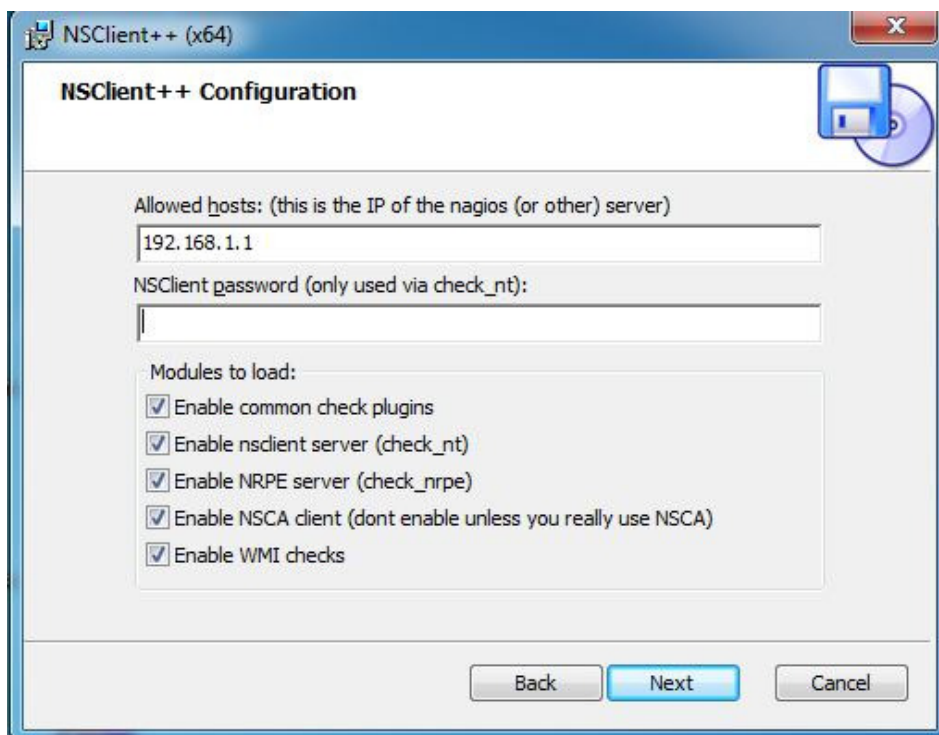
หมายเหตุ: สามารถ Download NSClient++ ได้ที่ <http://sourceforge.net/projects/nscplus/>

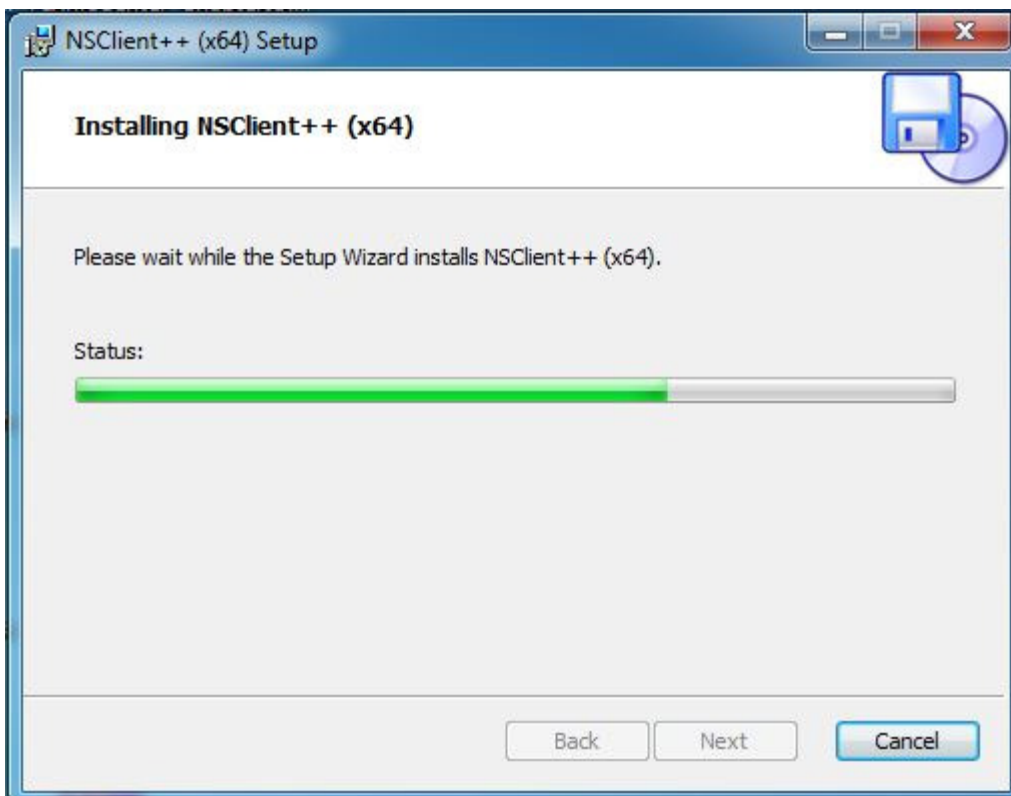
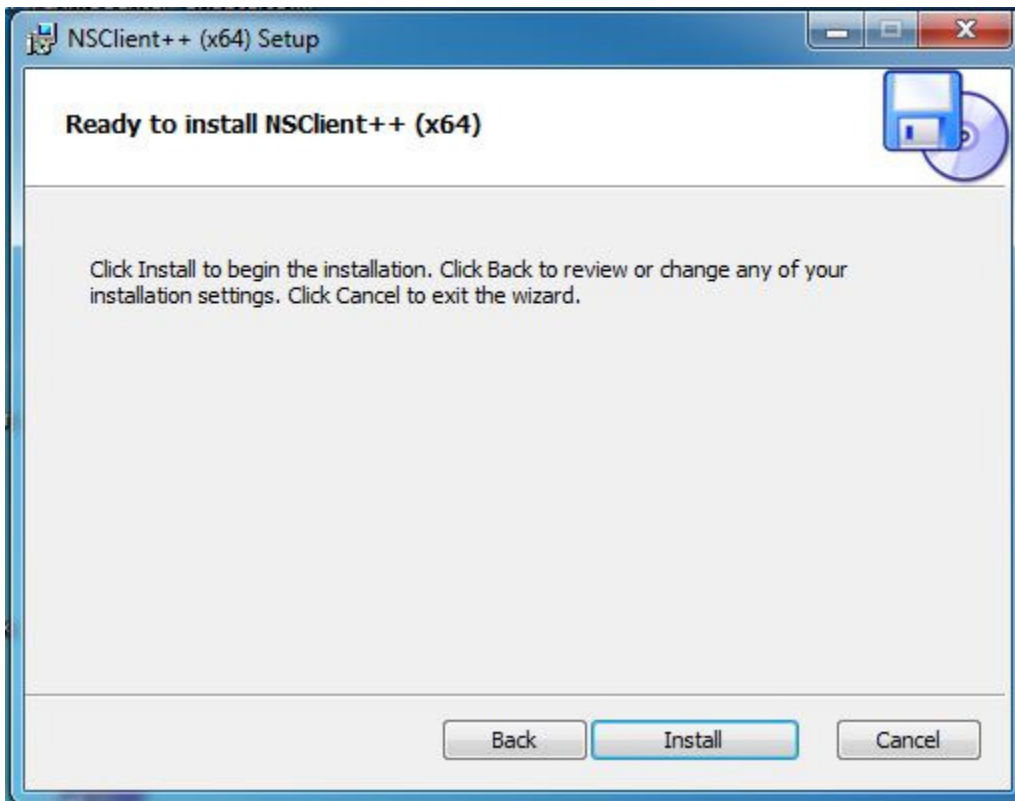
5.1 ติดตั้ง NSClient++



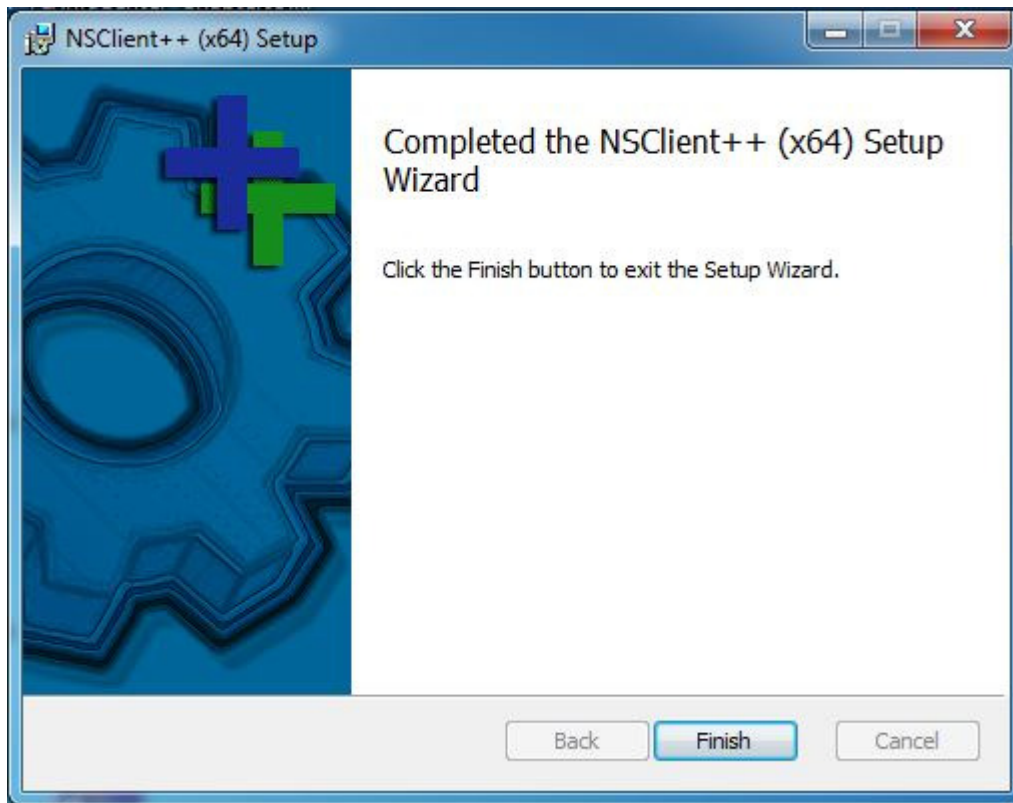


- ใส่ Nagios Server IP ส่วน Password ให้เว้นว่างไว้คลิก Next





- เสร็จสิ้นการติดตั้ง NSClient++



5.2 เริ่ม Configure Nagios Server

```
# vi /etc/nagios/nagios.cfg
```

และ uncomment ตามบรรทัดด้านล่าง

```
## Line 52 - Uncomment ##
```

```
cfg_dir=/etc/nagios/object/window.cfg
```

บันทึกไฟล์

```
# vi /etc/nagios/object/nagios.cfg
```

5.3 แก้ไข Change the Windows Client IP

```
define host{
    use                windows-server    ; Inherit default values from a template
    host_name          winserver         ; The name we're giving to this host
    alias              My Windows       ; A longer name associated with the host
    address            10.0.0.3         ; IP address of the host
}
```

5.4 ทำการเพิ่ม Service เหมือนของ Linux แต่ให้เปลี่ยนชื่อ host_name ให้เป็นของ Windows client ที่เราได้ตั้งไว้

5.5 จากนั้นทำการ Restart Nagios ด้วยคำสั่ง `# /etc/nagios restart` เป็นอันเสร็จสิ้น

ขั้นตอนที่ 6 การ Monitoring

6.1 หลังจากแก้ไขตามเอกสารด้านบนแล้ว ไปที่ [http://\(Server IP ที่ตั้งไว้\)/nagios](http://(Server IP ที่ตั้งไว้)/nagios) ใ้ username และ password หลังจากคลิกเมนู Host จะเห็นตามภาพด้านล่าง สีเขียว จะแสดงถึง Node ที่กำลังทำงาน

The screenshot shows the Nagios Core web interface in Mozilla Firefox. The browser address bar shows `localhost/nagios/`. The interface displays the following data:

Current Network Status
 Last Updated: Sun Nov 2 10:54:21 ICT 2014
 Updated every 90 seconds
 Nagios® Core™ 3.5.1 - www.nagios.org
 Logged in as nagiosadmin

Host Status Totals

Up	Down	Unreachable	Pending
3	0	0	0

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
15	1	0	7	0

Host Status Details For All Host Groups

Limit Results: 100

Host	Status	Last Check	Duration	Status Information
client	UP	11-02-2014 10:53:28	0d 0h 1m 13s	PING OK - Packet loss = 0%, RTA = 0.80 ms
localhost	UP	11-02-2014 10:52:48	6d 15h 32m 41s	PING OK - Packet loss = 0%, RTA = 0.05 ms
winsrvr	UP	11-02-2014 10:51:48	0d 0h 2m 53s	PING OK - Packet loss = 0%, RTA = 0.51 ms

Results 1 - 3 of 3 Matching Hosts

6.2 สามารถตรวจสอบ Service ต่างๆในแต่ละ Node ได้ด้วยการคลิกที่ชื่อของ Node นั้นๆ ตามภาพด้านล่าง

The screenshot shows the Nagios Core web interface in Mozilla Firefox. The browser address bar shows `localhost/nagios/`. The interface displays the following data:

Current Network Status
 Last Updated: Sun Nov 2 10:55:21 ICT 2014
 Updated every 90 seconds
 Nagios® Core™ 3.5.1 - www.nagios.org
 Logged in as nagiosadmin

Host Status Totals

Up	Down	Unreachable	Pending
1	0	0	0

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
4	0	0	3	0

Service Status Details For Host 'winsrvr'

Limit Results: 100

Host	Service	Status	Last Check	Duration	Attempt	Status Information
winsrvr	C:\ Drive Space	OK	11-02-2014 10:51:15	0d 0h 4m 6s	1/3	c - total: 204.98 Gb - used: 100.20 Gb (49%) - free 104.78 Gb (51%)
winsrvr	CPU Load	CRITICAL	11-02-2014 10:50:20	0d 1h 25m 1s	1/3	Network is unreachable
winsrvr	Explorer	OK	11-02-2014 10:51:25	0d 0h 3m 56s	1/3	explorer.exe: Running
winsrvr	Memory Usage	OK	11-02-2014 10:52:29	0d 0h 2m 52s	1/3	Memory usage: total:16119 99 Mb - used: 3240.24 Mb (20%) - free: 12879.75 Mb (80%)
winsrvr	NSClient++ Version	CRITICAL	11-02-2014 10:45:34	0d 1h 19m 47s	2/3	CRITICAL - Socket timeout after 10 seconds
winsrvr	Uptime	OK	11-02-2014 10:54:39	0d 0h 0m 42s	1/3	System Uptime - 0 day(s) 2 hour(s) 29 minute(s)
winsrvr	W3SVC	CRITICAL	11-02-2014 10:45:43	0d 18h 5m 5s	3/3	CRITICAL - Socket timeout after 10 seconds

Results 1 - 7 of 7 Matching Services

6.3 แถบสีแดงจะแสดงถึง Node ที่หยุดทำงานแล้ว

Nagios
 Current Network Status
 Last Updated: Sun Nov 2 10:41:27 ICT 2014
 Updated every 30 seconds
 Nagios® Core™ 3.5.1 - www.nagios.org
 Logged in as nagiosadmin

Host Status Totals

Up	Down	Unreachable	Pending
1	2	0	0

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
10	1	0	12	0

Host Status Details For All Host Groups

Limit Results: 100

Host	Status	Last Check	Duration	Status Information
client	DOWN	11-02-2014 10:39:38	0d 1h 5m 49s	CRITICAL - Host Unreachable (192.168.1.4)
localhost	UP	11-02-2014 10:37:18	6d 15h 19m 47s	PING OK - Packet loss = 0%, RTA = 0.06 ms
winserver	DOWN	11-02-2014 10:41:08	0d 0h 56m 59s	CRITICAL - Host Unreachable (192.168.1.6)

Results 1 - 3 of 3 Matching Hosts