

# Nagios Network Monitör Uygulaması -2

Erkan Esmer

Nisan, 2016

# İçindekiler

1	Monitoring Sistemleri . . . . .	2
2	Nagios'a Windows Sunucu Ekleme . . . . .	3
3	Nagios'a Linux Sunucu Ekleme . . . . .	6

# 1 Monitoring Sistemleri

Geçen sayıdaki yazımızda Nagios'u kurup çalışma mantığına bakmıştık. Bu sayımızda ise izlemek istediğimiz cihazları Nagios'a ekleyeceğiz. "Bunu yapmak için neler yapmak gerekir?" sorusuna cevaplar arayarak yazımızı sürdüreceğiz ve Nagios yazımız tamamlanmış olacak.

Geçen ay kurduğumuz Nagios uygulamamıza web arayüzünden aşağıdaki şekilde ulaşabiliriz.

[http://nagios-sunucu\\_ap-adresi/nagios/](http://nagios-sunucu_ap-adresi/nagios/)



Şekil 1:

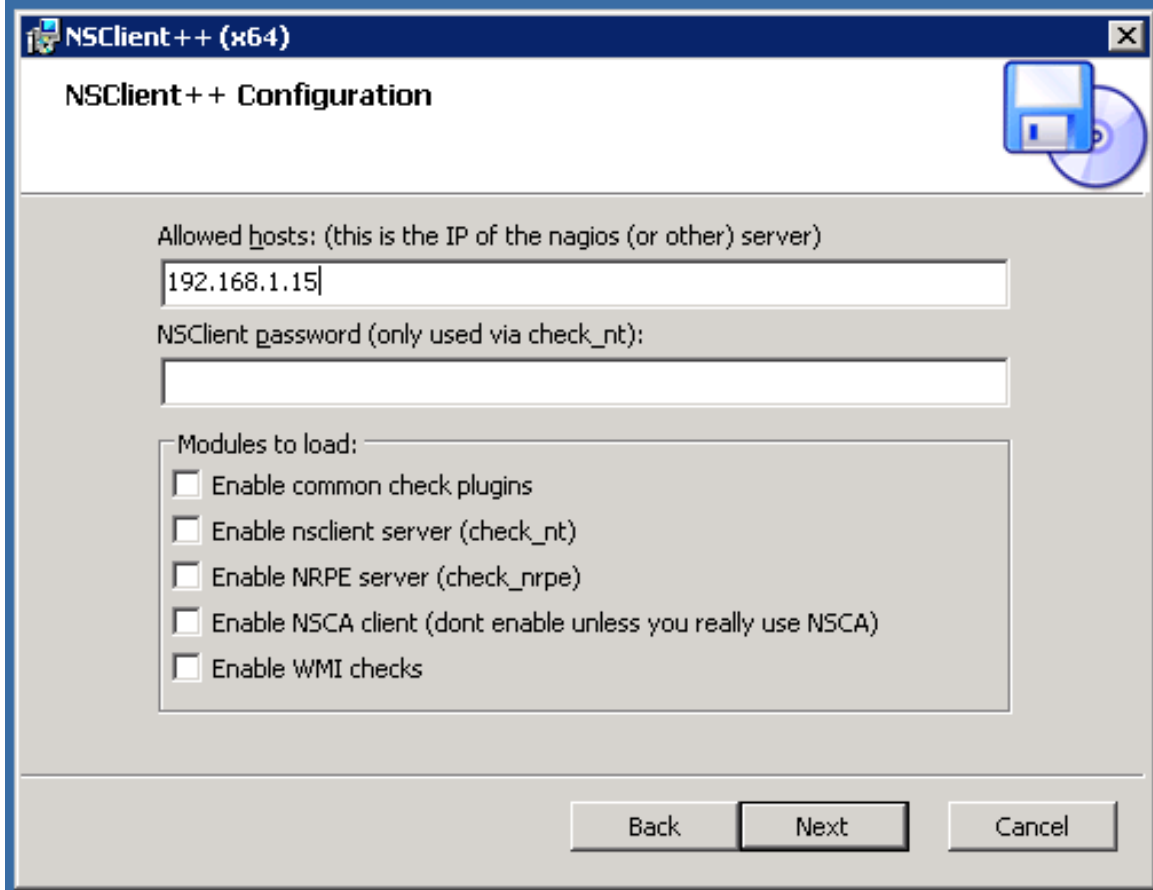
Şu an için Nagios sunucumuzda izlediğimiz herhangi bir sunucumuz yok. Bu yazımızda Windows ve Linux sunucularımızı Nagios'a ekleyip izleme başlatacağız.

## 2 Nagios'a Windows Sunucu Ekleme

Nagios istenilen cihazda izleme yapabilmesi için karşı tarafta bir agent kurulmasını ister. Windows Sistemler için NSClient++ uygulamasını kurarak Nagios ile bağlantıyı sağlayacağız.

İlk önce aşağıdaki adresten terminal uygulamamızı indiriyoruz. Bu bağlantıda sisteminize uygun olan sürümü (32Bit-64Bit)seçebilirsiniz.

<http://sourceforge.net/projects/nscplus/files/nscplus/NSClient%2B%2B%200.4.1/>



Şekil 2:

Kurulumda önemli olan nokta yan gördüğümüz ekran. Burada Allowed Hosts alanına Nagios sunucumuzun IP adresini giriyoruz.

Böylece NSClient yüklü sunucu üzerinde Nagios sunucumuz izinli oluyor ve izleme yapabilir durumda olabiliyor.

Bu kurulumla izlenecek cihaz tarafında gereklilikleri yapmış olduk.

Şimdi Nagios tarafında ayarlara bakalım.

Nagios kurulumu ile beraber gelen .cfg dosyalarından windows.cfg dosyası, Windows sunucular için bize bir şablon dosya görevini görebilir. Bu dosyayı örnek alarak Windows sunucumuza uyarlayabiliriz.

Nagios sunucumuzda /etc/nagios/object klasörünün içine giriyoruz. Object klasörü içinde windows.cfg dosyasını bulup bir kopyasını çıkartabiliriz. Bu kopya dosyamızı Windows sunucumuz için kullanacağız. Kopyalamak için; /etc/nagios/object klasörü içindeyken;

```
1 cp windows.cfg windowsServer-1.cfg
```

Şimdi yeni dosyamız windowsServer-1.cfg dosyamızı editleyelim. Editleme için vim ya da nano'yu kullanabiliriz. /etc/nagios/object klasörü içindeyken

```
1 vim windowsServer-1.cfg veya nano windowsServer-1.cfg
```

Dosyayı açtığımızda 3 önemli tanımlama alanından oluştuğunu göreceğiz.

```
1 Define_Host
2 Define_HostGroup
3 Define_Services
```

Define\_Host alanında sunucumuzun erişim bilgilerini tanımlıyoruz. Aşağıda ekran görüntüsünü görmekteyiz.

```
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 Server ; A longer name associated with the host
    address            192.168.1.2    ; IP address of the host
}
```

Şekil 3:

İzleyeceğimiz Windows sunucumuzun host\_name tanımını ve ip\_adresi tanımı yaptık.

Ardından Host\_Group alanında ise bu hostumuzu hangi grupta tutacağımızı belirtiyoruz.

Nagios arayüzünde izlediğimiz cihazları grup bazlı ayırabilir ve monitörleyebiliriz.

Önemli bir detay olarak belirtmekte fayda var. Bir Host\_Group sadece bir .cfg dosyasında belirtilir. Birden fazla olması durumunda Nagios servisi başlatılırken hata alırız. Sonuç olarak Host\_Group'u tanımlıyoruz ve bu gruba giren diğer cihazları da define\_host tarafındaki use alanına tanımlıyoruz. Aşağıdaki çıktıda gördüğümüz gibi Host\_Group tanımlamasını yaptık.

```
define hostgroup{
    hostgroup_name    windows-servers ; The name of the hostgroup
    alias             Windows Servers ; Long name of the group
}
```

Şekil 4:

Son olarak bu cihaz üzerinde kontrol edeceğimiz servislerin tanımları var.

Servisler kısmında kurulumla birlikte gelen .cfg dosyasında toplam 7 adet servis bulunmaktadır. 1 tanesi monitörlenen makineye kurulan uygulamanın versiyonunu kontrol eder. Diğerleri ise mesela ekranda gördüğümüz üzere Uptime süresi, Cpu kullanımı ve devamında ram, disk kullanımını izleyen servisler vardır. Bunları kaldırabileceğimiz gibi eklemeler de yapabiliriz.

Monitörlenen makinenin .cfg dosyasında değineceğimiz temel başlıklar bu kadar. Böylece .cfg dosyasıyla işimiz tamamlanmış oldu. Şimdi Nagios'a bu cihazın .cfg dosyasını göstererek izleme işlemini başlatabiliriz. Bunun için /etc/nagios klasöründeki nagios.cfg dosyasına aşağıdaki gibi bir girdi yapmamız gerekir.

Böylece sunucumuza göre uyarladığımız .cfg dosyamızın yolunu Nagios'a da bildirmiş olduk. Artık Nagios ilgili sunucumuzu monitör edecektir. Arayüzde Host alanında görebiliriz.

```

define service{
    use                generic-service
    host_name          winserver
    service_description Uptime
    check_command       check_nt!UPTIME
}

# Create a service for monitoring CPU load
# Change the host_name to match the name of the host you defined above

define service{
    use                generic-service
    host_name          winserver
    service_description CPU Load
    check_command       check_nt!CPULOAD!-1 5,80,90
}

```

Şekil 5:

```

# Definitions for monitoring a Windows machine
#cfg_file=/etc/nagios/objects/windows.cfg
cfg_file=/etc/nagios/objects/windowsServer-1.cfg

```

Şekil 6:

### 3 Nagios’a Linux Sunucu Ekleme

Linux sunucumuz için de aynı Windows sunucumuzda olduğu gibi Nagios bir agent uygulama istiyor. Linux sunucular için NRPE uygulamasını kullanacağız. Bu uygulama sayesinde Nagios sunucumuz üzerinde izleme yapabilecek.

Uygulamayı yüklemek için terminal penceresinden

```
1 yum install nagios-nrpe
```

komutunu vermemiz gerekiyor. \*Bu komut Centos sistemler için geçerlidir. Debian için de

```
1 apt-get install nagios-nrpe
```

dememiz gerekiyor.

Bu arada rpmforge veya epel repolarının sistemimize yüklü olduğunu varsayıyoruz. Aksi hâlde kurulumla gelen repolarda bu uygulamayı bulamayız.

Kurulum tamamlandıktan sonra /etc/nagios klasörü altında nrpe.cfg dosyasını bulabiliriz. Bu dosyayı editleyip allowed\_hosts alanının karşısına Nagios sunucumuzun ip adresini yazıyoruz.



Şekil 7:

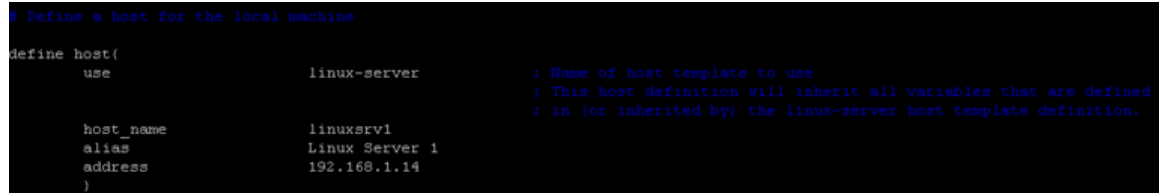
Ardından nrpe servisini yeniden başlatarak (/etc/init.d/nrpe restart) monitörlenecek sunucumuz tarafında işlemlerimizi tamamlıyoruz.

Şimdi Nagios tarafında yapacaklarımıza bakalım. Tıpkı Windows sunucumuz için yaptığımız gibi Linux sunucumuz için de bir .cfg dosyası oluşturacağız. Bunun için örnek dosya olarak /etc/nagios/object klasörü altındaki localhost.cfg dosyayı kullanacağız. Localhost.cfg dosyası Linux sunucular için şablon dosya olarak kullanılabilir. Bu dosyayı kendi sunucumuza göre uyarlayacağız.

Yine .cfg dosyasında Define\_Host, Define\_HostGroup, Define\_Services alanlarını göreceğiz.

Define\_Host alanına erişim bilgilerimizi HostGroup alanına Linux sunucumuzu ekleyeceğimiz grubu tanımlayacağız. Yine Windows sunucumuzda yaptığımız gibi hareket ediyoruz.

Aşağıdaki çıktıda da göreceğimiz gibi use alanına grubu, host\_name alanına makine adını, alias alanına arayüzdeki görünecek adını ve address alanına da sunucumuzun IP adresini yazıyoruz.



Şekil 8:

Host\_Group alanını tekrar olmaması açısından Windows sunucularla aynı olduğu için geçip Define\_service alanından bir çıktıyı inceleyelim.

```

define service{
    use                local-service        ; Name of service template to use
    host_name          linuxsrv1
    service_description Total Processes
    check_command       check_local_procs!250!400!RSZDT
}

# Define a service to check the swap usage the local machine.
# Critical if less than 10% of swap is free, warning if less than 20% is free

define service{
    use                local-service        ; Name of service template to use
    host_name          linuxsrv1
    service_description Swap Usage
    check_command       check_local_swap!20!10
}

# Define a service to check SSH on the local machine.
# Disable notifications for this service by default, as not all users may have SSH enabled.

define service{
    use                local-service        ; Name of service template to use
    host_name          linuxsrv1
    service_description SSH
    check_command       check_ssh
    #notifications_enabled 0
}

```

Şekil 9:

Total\_Processes, Swap\_Usage ve SSH servislerinin tanımını görmekteyiz. Bu tanımlar sayesinde arayüzde ilgili servisleri monitör edebileceğiz. İstediklerimizi kaldırabilir takip etmek istediğimiz servis için de tabii ki eklemeler yapabiliriz.

Son olarak Nagios tarafında /etc/nagios/nagios.cfg dosyasına Linux sunucumuz için uyarladığımız dosyamızı tanımlıyor ve Linux sunucumuz için de izlemeyi başlatıyoruz. Tabii değişikliklerin etkin olması için Nagios servisini tekrar başlatmamız gerekiyor. /etc/init.d/nagios restart

```

# Definitions for monitoring the local (Linux) host
cfg_file=/etc/nagios/objects/linux-server1.cfg
cfg_file=/etc/nagios/objects/localhost.cfg

```



Şekil 10:

Tüm bu işlemlerden sonra [http://nagios-sunucu\\_ap-adresi/nagios/](http://nagios-sunucu_ap-adresi/nagios/) şeklindeki bağlantımızı kullanarak Nagios arayüzüne ulaşabiliriz. İşte eklediğimiz sunucularımız da monitör edilmekte.

Nagios'ta temel olarak yaptığımız işlemlere değinip 2 çeşit sunucumuzu da ekledik.

Görüşmek üzere.



C:\ Drive Space	OK	06-11-2013 17:08:51	0d 4h 20m 15s	1/3	c: - total: 39.90 Gb - used: 29.02 Gb (73%) - free 10.88 Gb (27%)
CPU Load	OK	06-11-2013 17:08:02	0d 4h 21m 4s	1/3	CPU Load 17% (5 min average)
Explorer	OK	06-11-2013 16:59:13	15d 6h 29m 56s	1/3	explorer.exe: Running
Memory Usage	WARNING	06-11-2013 17:00:24	15d 6h 28m 45s	3/3	Memory usage: total:6445.36 Mb - used: 5509.12 Mb (85%) - free: 936.23 Mb (15%)
NSClient++ Version	OK	06-11-2013 17:01:35	15d 6h 27m 34s	1/3	NSClient++ 0,4,1,73 2012-12-17
Uptime	OK	06-11-2013 17:04:47	11d 13h 44m 19s	1/3	System Uptime - 132 day(s) 22 hour(s) 40 minute(s)
WGSVC	CRITICAL	06-11-2013 17:04:33	43d 2h 1m 12s	3/3	WGSVC: Not found
Current Load	OK	06-11-2013 17:05:45	42d 7h 12m 25s	1/4	OK - load average: 0.43, 0.20, 0.12
Current Users	OK	06-11-2013 17:06:55	42d 7h 11m 47s	1/4	USERS OK - 1 users currently logged in
HTTP	 WARNING	06-11-2013 17:08:06	41d 16h 51m 10s	4/4	HTTP WARNING: HTTP/1.1 403 Forbidden - 5237 bytes in 0.002 second response time
PING	OK	06-11-2013 17:04:18	42d 7h 15m 32s	1/4	PING OK - Packet loss = 0%, RTA = 0.06 ms
Root Partition	OK	06-11-2013 17:05:29	42d 7h 14m 55s	1/4	DISK OK - free space: / 43144 MB (94% inode=97%);
SSH	 OK	06-11-2013 17:06:40	42d 7h 14m 17s	1/4	SSH OK - OpenSSH_5.3 (protocol 2.0)
Swap Usage	OK	06-11-2013 17:07:51	42d 7h 13m 40s	1/4	SWAP OK - 100% free (2015 MB out of 2015 MB)
Total Processes	OK	06-11-2013 17:04:37	42d 7h 13m 1s	1/4	PROCS OK: 69 processes with STATE = RSZDT

Şekil 11: