

Nagios Network Monitör Uygulaması

Erkan Esmer

Nisan, 2016

İçindekiler

1	Monitoring Sistemleri	2
2	Nagios Network Monitör Uygulaması	3
3	Nagios'un Çalışma Şekli	4
4	Nagios Kurulumu	5
4.1	Kuruluma Hazırlık ve Kurulum Adımları	5

1 Monitoring Sistemleri

Not: Nagios çalışmasını Centos sunucu üzerinde yapmış olduğumuzdan dolayı kurulum ve yapılandırma tarifi Centos'a göredir.
{: .onemli}

2 Nagios Network Monitör Uygulaması

Nagios, bir sistem ve ağ denetleme uygulamasıdır. Sunucu olarak belirlediğimiz makineye Nagios'u kurup izlemek, denetlemek istediğimiz makineye de agent (ajan) uygulamasını kurup gerekli konfigürasyonu yapar ve Nagios'u çalıştırırız.

Genel olarak Nagios ile neler yapabiliriz?

1. Ağ üzerinde istenilen makinelerin servislerini monitör edebilme. (Smtplib, pop3, http, ping vs.)
2. Makinelerin kaynaklarının durumlarını izleyebilme. (Disk kullanımı, İşlemci kullanımı vs.)
3. Makine kaynaklarında veya servislerinde oluşabilecek durumlara karşı e-posta, SMS aracılığı ile bilgilendirme yapabilme.
4. Network haritası çıkarabilme.
5. Web arayüzü ile takip yapabilme ve rapor alabilme.

Nagios'un diğer sağladıkları ve detaylar için www.nagios.org adresine bakabilirsiniz.

3 Nagios'un Çalışma Şekli

Nagios, uygulama olarak kurulduğu host makinede çalışır. Nagios'un üzerinde tanımlı pluginler vardır. Bu pluginler kurulumla beraber gelir. Kurulum sonrası monitör edilecek cihazları ".cfg" dosya türü ile Nagios'a tanımlarız (Nagios klasörünün altındaki object klasörü içine). Yani her izlenen cihazın bir .cfg uzantılı tanımlama dosyası olur. Bu tanımlama dosyaları da Nagios'un konfigürasyon dosyasında (Nagios klasöründe içindeki nagios.cfg dosyası) gösterilir.

Buna göre Nagios kendisinde tanımlı .cfg dosyaları sayesinde hangi ağ üzerindeki hangi cihazda hangi komutları çalıştıracağını bilir. Ayrıca çalıştıracağı komutlar da yine Nagios klasörünün altındaki object klasörünün içinde command.cfg dosyasında tutulur.

Sonuç olarak Nagios monitör ettiği cihazlarda birtakım pluginler çalıştırır. Bu pluginler de aslında komutlardan oluşur. Nagios çalıştırdığı pluginler sayesinde izlediği makineden bilgileri toplar ve bir web arayüzünde sunar.

Tabii bir de Nagios'un yukarıda bahsettiğimiz komutları karşı tarafta çalıştırabilmesi için eğer Unix/Linux makineyse NRPE eklentisini kurmak eğer Windows ise NSClient++ eklentisini kurmak gerekir. Bu eklentileri kurarak Nagios'un makinelere erişerek gerekli komutları çalıştırabilmesini sağlamış oluruz.

Nagios, **5666** numaralı port ile haberleşir.

4 Nagios Kurulumu

4.1 Kurulum Hazırlık ve Kurulum Adımları

Öncelikle Nagios kurulumu için sistemimize repo ekleyeceğiz. Böylece eklediğimiz repodan Nagios ve Nagios-Plugin kurulumlarını yapacağız. Ayrıca web arayüzü için de Apache kurulumu yapacağız.

Yani maddelendirirsek;

1. repo ekleme
2. Apache kurulumu
3. Nagios ve Nagios-Plugin kurulumu

En etkin repolar olan rpmforge ve epel repolarını veya birini sistemimize eklemek kurulum için yeterli. Bunun için biz şöyle bir yol izleyeceğiz. Tabii ki başka yöntemler de vardır.

Linux paketlerini arayıp indirebileceğimiz başarılı bir kaynak site olan pkgs.org sitesine girip arama alanından epel kelimesi aratalım. Çıkan sonuç aşağıdaki gibi olacaktır.

EPEL:

- [epel-release-6-8.noarch.rpm](#) - Extra Packages for Enterprise Linux repository configuration

Şekil 1:

Bağlantıya tıkladığımızda açılan sayfada nasıl kuracağımıza dair yönlendirmeyi göreceğiz.

Install Howto

1. Download the latest epel-release rpm from

```
http://dl.fedoraproject.org/pub/epel/6/i386/
```

2. Install epel-release rpm:

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

3. Install epel-release rpm package:

```
# yum install epel-release
```

Şekil 2:

Epel-release dosyasını indirip aynı konumdayken;

```
1 rpm -Uvh epel-release
```

komutunu vermemiz epel reposunun kurulumu için yeterlidir. Artık kurulum isteklerimiz epel reposundan da arattırılacaktır.

Son olarak Nagios kurulumuna başlamadan önce sistemimizde yoksa

```
1 yum install httpd
```

komutu ile Apache kurulumunu yapıyoruz. Apache ile ilgili sadece Nagios için kullanacağımız için ek ayarlar yapmayacağız. Kurulum yapmamız yeterli. Ardından

```
1 yum install nagios
```

komutunu veriyor ve Nagios kurulumu yapıyoruz.

Kurulum tamamlandıktan sonra /etc/nagios yoluna Nagios uygulamasının kurulduğunu görebilirsiniz. Şimdi Nagios dizinine bir bakalım.

```
[root@nagios ~]# ls
cgi.conf  conf.d  nagios.conf  objects  passwd  private
[root@nagios ~]#
```

Şekil 3:

Buradaki dosya ve klasörler Nagios yapılandırılmasında kullanılan içerikleri ve dosyaları barındırır. Bunlara bakalım; cgi.conf Bu dosyada web arayüzü için ayarlar bulunur. Temelde barındırdığı ayarlarla kullanabiliriz. Şimdilik bu dosyada ek bir şey yapmaya gerek yok. Nagios.conf Bu dosya ile monitör edeceğimiz cihazların önceden yaptığımız .cfg dosyalarının yolunu belirtiriz. Böylece Nagios belirtilen .cfg dosyalarına göre monitörleme yapmaya başlar.

Passwd Kurulum sonrası web arayüz erişimi için KullanıcıAdı:nagiosadmin Şifre:nagiosadmin olarak gelir. Bu dosya şifrenin tutulduğu dosyadır.

Private Klasörü Private klasörü içinde resource.cfg dosyasını barındırır. Resource.cfg dosyası da Nagios Plugin dosyalarının yolunu tutar. Nagios bir plugin çalıştıracağı zaman plugin dosyasını bu dosyada belirtilen konumda arar.

Objects Klasörü Bu klasörde monitör ettiğimiz cihazların konfigürasyon dosyaları ve çalıştıracağımız komutların dosyası tutulur. İçerisinde localhost.cfg dosyasını windows.cfg dosyasını switch.cfg dosyasını görmekteyiz.

Örneğin windows.cfg dosyasına bir bakalım.

```
define host {
    use                windows-server ; Inherit default values
    host_name          winserver      ; The name we're giving t
    alias              My Windows Server ; A longer name a
the host
    address            192.168.1.2    ; IP address of the host
}
```

Şekil 4:

Dosyayı açtığımızda “Host Definitions” başlığı altında “define host { }” parantezler arasına monitör edeceğimiz Windows makinenin Grubunu (WindowsServer Grup diyebiliriz. WebArayüzde Windows grubu görmemizi sağlar.) Makine adını ve en önemlisi address başlığı karşısına ip_adresini yazarız.

Yukarıdaki girdilere göre ip_adresi 192.168.1.2 olan, adı winserver olan bir sunucumuzu windows-server grubunun içine monitör etmek üzere belirtmiş olduk.

Devam ediyoruz;

```
# Define a host group for Windows machines
# All hosts that use the windows-server template will automatically be
of this group

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

Şekil 5:

Yukarıda bahsettiğimiz grup tanımının yapıldığı alan.

Unutmayalım! Eğer windows-servers grubu oluşturup bu grup altına sunucuları koyuyorsak bu grup tanımını sadece ilk oluşturduğumuz dosyada yapacağız. İlk dosya ile beraber grup tanımı yapılmış olacak. Diğer dosyalarda yukarıda değindiğimiz gibi sadece üye olduğu grubu belirteceğiz.

Aksi hâlde her dosyada bir grup tanımlamaya çalışırsak aynı isimli grup olacağından hata alırız.

Yine windows.cfg dosyasında devam ediyoruz. Aşağıda iki adet servis tanımı görmekteyiz. Biri UPTIME girdisi ile sunucunun uptime zamanına bakmakta diğeri ise CPULOAD girdisi ile işlemci yüküne bakmakta. Bunları aşağıda görülen formatta dilediğimiz kadar çoğaltabilir ve sunucunun istediğimiz servisini veya durumu izlemeye alabiliriz.

```
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 -l 5, 80, 90
}
```

Şekil 6:

İşte windows.cfg dosyasını Windows olan her sunucumuz için kullanabiliriz. Diğer dosyalar da adından da anla-

şılacağı üzere switch.cfg, switch kontrolleri için printer.cfg dosyası printer cihazların kontrolleri için şablon .cfg dosyalarıdır. Bu dosyaları cihazlarımıza göre özelleştirerek kullanabiliriz.

Örneğin yukarıda içeriğine baktığımız windows.cfg dosyasını içeriğini düzenleyip adını da sunucumuz ismini vererek kaydeder ve kullanabiliriz. Örn:FileServer-1

Son olarak bu .cfg dosyasının yolunu /etc/nagios/ altında bulunan nagios.cfg dosyasına ekliyoruz.

```
# You can specify individual object config files as shown below
cfg_file=/etc/nagios/object/commands.cfg
cfg_file=/etc/nagios/object/contacts.cfg
cfg_file=/etc/nagios/object/templates.cfg
cfg_file=/etc/nagios/object/templats.cfg

# Definitions for monitoring the local (Linux) host
cfg_file=/etc/nagios/object/localhost.cfg

# Definitions for monitoring a Windows machine
#cfg_file=/etc/nagios/object/windows.cfg

# Definitions for monitoring a router/switch
#cfg_file=/etc/nagios/object/switch.cfg

# Definitions for monitoring a network printer
#cfg_file=/etc/nagios/object/printer.cfg
```

Şekil 7:

Nagios yukarıda da anlattığımız gibi .cfg dosyasına ulaşarak, içeriğine göre izlemeyi başlatıyor.

Mesela kendi oluşturduğumuz dosyanın adını FileServer-1.cfg olarak vermiş olalım. nagios.cfg dosyasında oluşacak girdi aşağıdaki gibi olacak.

```
# Definitions for monitoring a Windows machine
#cfg_file=/etc/nagios/object/windows.cfg
cfg_file=/etc/nagios/object/FileServer-1.cfg
```

Şekil 8:

Temel olarak Nagios Sunucusunda yapacağımız ayarlar ve düzenlemelere değindik. Bir de izlenecek tarafta izlemenin sağlanabilmesi için eklenti bir uygulama kurulması gerekiyor.

Windows sunucular için <http://sourceforge.net/projects/nscplus/> adresinden NSClient++ kurulumunu indiriyoruz ve sunucuda kuruyoruz. Kurulum sırasında bize Nagios sunucunun ip adresi soruluyor. Bu bilgiyi de girdiğimizde ve kurulum tamamlandığında izlenecek makine izlenmeye hazır duruma geliyor. Monitör edilecek makine tarafında başka bir ayar yapmamıza gerek yok. Yalnız kurulumun başarılı şekilde tamamlandığını kontrol etmek için şunu yapabiliriz.

Windows komut satırında;

```
1 netstat -an | find /i "":5666 komutunu çalıştırır ve LISTENING dönüşü alırsak problem yok  
demektir .  
2 **Nagios 5666 portundan çalışır .
```

Eğer Linux bir makineyi monitor edeceksek aynı Windows makineye kurduğumuz gibi bir uygulamayı da Linux makinemize kuruyoruz.

Yum install nagios-nrpe komutu ile kurulumu yapıyoruz. Kurulum bittikten sonra /etc/nagios/ klasörü altına nrpe.cfg dosyasının geldiğini göreceğiz. Bu dosyayı edit edip AllowedHosts tanımına Nagios Server makinenin ip_adresini girmemizle monitörleme için karşı cihazda gerekenleri yapmış oluruz.

Yine kontrol için terminal penceresinde;

```
1 netstat -an | grep 5666 komutunu çalıştırdığımızda LISTEN sonucunu alırsak kurulum başarılı  
demektir .
```

Bu ayki yazımızda Nagios için kurulum ve yapılandırma yaptık. Temel olarak çalışır duruma getirdik. Önümüzdeki ay yine Nagios'tan devam ederek bir senaryo işleteceğiz. Windows, Linux makinelerimizi monitörlemeye alacak bunun yanına switch izleme de eklemeye çalışacağız. Bu çalışmayı da tamamlayınca web arayüzden Nagios uygulamamızı kullanacağız.

Görüşmek üzere...