MRTG KURULUMU VE KONFİGÜRASYONU

By Seyhan TEKELİOĞLU

seyhan@hotmail.com - http://www.seyhan.biz

Bu yazımda sizlere adım adım MRTG programının kurulumunu ve kullanımını anlatmaya çalışacağım.

Bölüm 1 : NT işletim sistemi üzerine MRTG Kurulumu

Kurulum (Installation) :

Web server olarak tanımlanmış, üzerinde IIS x.x. bulunan bir makineye mrtg kurulumu yapılabilir. Mrtg programı asıl olarak unix tabanlı makinelerde kullanılmak üzere tasarlanmıştır ve kodları perl diliyle yazılmıştır. NT tabanlı bir makinede mrtg çalıştırabilmek için işletim sistemine perl dilinin tanıyabilecek bir program kurmak gerekir. Bu program **Active Perl** dür. Active Perl'ü kurarken perl binary dizini system path'i olarak *C:\Perl\bin;%SystemRoot%\system32;%SystemRoot%;...* şeklinde bir tanımlama yapılmalıdır. System parh'I control etmek için [Control Panel]->[System]->[Environment] bölümüne bakabilirsiniz. Active Perl kurulduktan sonar mrtg'nin son sürümünü sisteme kurulmak için hazır hale geliriz. Bu yazı hazırlanırken mrtg-2.10.13 sürümü vardı. Kurulum aşamaları bu sürüme göre anlatılacaktır.

Şimdi yapacağımız işlem mrtg-2.10.13.zip dosyasını *C:\mrtg-2.10.13* dizini altına açmak olacaktır. Eğer buraya kadar sorunsuz bir şekilde her şeyi yaptıysak işlerin yolunda gittiğine dair küçük bir test yapabiliriz. Bunun için komut satırında düşüp *c:\mrtg-2.10.13\bin* dizini altına girin. Daha sonar *perl mrtg* komutunu çalıştırın. Karşınıza mrtg configuration dosyasını bulamadığına dair bir hata mesajı çıkacaktır. Henüz config. dosyamız yok ama mrtg sorunsuz bir şekilde sisteme kurulmuş durumda.

Ayarlar (Configuring) :

Mrtg konfigürasyonu yaparken önce bazı bilgileri toplamamız gerekli. Bu bilgiler bize conf. Dosyasını oluştururken yardımcı olacak. Şimdi madde madde gerekli bilgileri inceleyelim.

1 – Monitör etmek istediğimiz cihaza ait IP numarası, Hostname ve SNMP portu (Eğer standart port numarası değilse)

2 – Eğer farklı bir cihazı monitor etmek istiyorsanız (giriş çıkış byte'larını) o cihaza ait SNMPOID'yi bilmeniz gerekli.

3 – Son olarak monitor edeceğiniz cihaza ait read only SNMP community string'ini bilmeniz lazım. Eğer SNMP stringini değiştirilmediyse standart olarak *public* geçerlidir.

Oluşturacağımız örnek conf. dosyasını Cisco Catalyst 5000'e gore 10.10.10.1 ip numarasını ve public SNMP stringini kullanarak oluşturacağız. Yapacağımız ayarlar ile trafiği ve CPU yükünü monitor edeceğiz.

Konfigürasyona başlarken ilk adım cfgmaker ile mrtg.cfg dosyasını oluşturmak olacak. Bunu yapabilmek için komut satırına düşüp *c:\mrtg-2.10.13\bin* dizinine girin ve aşağıdaki komutu çalıştırın.

perl cfgmaker public@10.10.10.1 --global "WorkDir: c:\www\mrtg" --output mrtg.cfg

Bu komut sizing için bir mrtg.cfg dosyası oluşturacaktır. Router'ınız içindeki tüm interface'leri numara sırasına göre sıralanır. Malesef bu numaralar her router konfigürasyonu yaptığınızda değişir. Cfgmaker iel ilgili daha geniş bilgi ilerki konularda ayrıca anlatılacaktır. Bu komutu çalıştırdıktan sonra **no such name** veya **no response** hata mesajlarını alıyorsanız muhetmelen SNMP community stringinizi yanlış yazmışsınızdır. Kontrol edip komutu tekrar çalıştırmayı deneyin.

Conf.dosyasını inceleyecek olursak; # işareti ile başlayan satırlar açıklama yazılan satırları gösterir. DOS işletim sistemindeki REM komutu ile aynı işlevi görür.

Mrtg.cfg dosyasının en tepesinde *WorkDir: D:\InetPub\wwwroot\MRTG* satırı bulunur. Bu satır mrtg'nin web serverda bulunan yerini gösterir. Genellikle web kök dizininde bulunur. \InetPub\wwwroot\ altında bu dizin mevcut değilse oluşturmalısınız.

Örnek bir cfg dosyası aşağıdaki şekilde görünür.

```
################################################################## ########
# Description: LCP SUWGB
# Contact: Seyhan Tekelioglu
# System Name: LC-Bridge
# Location: Here

 #..... .....
```

Yukarıda belirtilen # ile başlayan açıklama satırlarıdır.

Target[10.10.10.1.1]: 1:public@10.10.10.1

Bu kısımı formüle edersek;

Hedef cihazın ip adresi : interface numarası : SNMP community string : ip adresi

İlk kısma hedef cihazın ip adresi yazılır. Interface numarası, cfgmaker ile tarama yaptığımızda bulduğumuz router içindeki interface'lere karşılık gelen numaradır. Bu numaralar interfacelerde konfigürasyon değişikliği yapıldığında değişebilir buna dikkat etmek gerekir. SNMP community stringi netrokümüz için verdiğimiz Read-Only SNMP adıdır. Standart olarak public gelir. Ip adresi kısmı ise monitor edilecek cihazın ip adresidir.

MaxBytes[10.10.10.1.1]: 1250000

Bu satırda interface hız tanımlaması yapılmaktadır. Standart hız 10 mbit tir. Bunu 100 mbit yapmak için verilecek değer 12500000 dir.

Title[10.10.10.1.1]: LC-Bridge (sample.device): ether0

Bu satırda web arabirimde görünecek başlık bilgisini bulunur.

PageTop[10.10.10.1.1]: <H1>Traffic Analysis for ether0</H1>
<TABLE>
<TR><TD>System:</TD><TD>LC-Bridge inAndover</TD></TR>
<TR><TD>Maintainer:</TD><TD>Seyhan Tekelioglu</TD></TR>
<TR><TD>Interface:</TD><TD>ether0(1) </TD></TR>
<TR><TD>IP:</TD><TD>sample.device(10 .10.10.1)</TD></TR>
<TR><TD>Max Speed:</TD>
<TD>1250.0 kBytes/s (ethernetCsmacd)</TD></TR>
</TABLE>
Target[10.10.10.1.2]: 2:public@10.10.10.1
MaxBytes[10.10.10.1.2]: 1250000
Title[10.10.10.1.2]: LC-Bridge (): ulink0
PageTop[10.10.10.1.2]: <H1>Traffic Analysis for ulink0</H1>
<TABLE>
<TR><TD>System:</TD><TD>LC-Bridge inAndover</TD></TR>
<TR><TD>Maintainer:</TD><TD>Seyhan Tekelioglu</TD></TR>
<TR><TD>Interface:</TD><TD>ulink0(2) </TD></TR>
<TR><TD>IP:</TD><TD>()</TD>< ; ; ;/TR>
<TR><TD>Max Speed:</TD>
<TD>1250.0 kBytes/s (ethernetCsmacd)</TD></TR>
</TABLE>
#-- ----

En basit şekliyle yukarıdaki gibi bir mrtg.cfg dosyası tanımlanabilir. Bu dosyayı çalıştırmak için komut satırından *c:\mrtg-2.10.13\bin* dizinine girip *perl mrtg mrtg.cfg* yazın. İlk iki çalıştırma işleminde hata mesajı almanız normaldir. Bu hatalar size daha once herhangi bir log dosyasının oluşmadığını haber verirler. Şu ana kadar yaptığımız işlemler bizim mrtg programımızı çalıştırır fakat düzenli bir web görüntüsü alamayız. Bunun için sistemi stabil ve akıcı bir şekilde belli aralıklarla (örneğin 5 dakikada bir) çalıştırmamız gerekli. Bunu nasıl yapacağımızı şimdiki bölümde bulabilirsiniz.

Mrtg Sürekli Çalışsın :

Mrtg programımızı 5 dk. Da bir manuel olarak çalıştırmak sanırım bir sure sonra bayağı bir sıkıcı hal alır. Bunun için çalıştırma olayını otomatiğe bağlasak bizim için daha mutluluk verici olur değil mi?

RunAsDaemon: yes

Bu özel ve güzel komutu mrtg config. dosyası içinde kullanarak hayatımızı daha da kolaylaştırabiliriz. Bu komutun mrtg scriptini çalıştırdıktan sonra kapatmayacak ve her 5 dakikada bir bu işlemyi yineleyecektir.

start /Dc:\mrtg-2.10.13\bin wperl mrtg --logging=eventlog mrtg.cfg

mrtg conf. dosyanızı yukarıdaki şekilde çalıştırmayı deneyin.

Eğer **perl** yerine **wperl** kullanırsanız karşınıza siyah konsol ekranı çıkmaz. Mrtg şu anda arka planda çalışmakta. Olası çıkabilecek problemleri **Event Log** içerisinden kontrol

edebilirsiniz. Bunu test için mrtg'ti durdurup Task Manager'ı açın, wper.exe dosyasını sonlandırdığınızda Event Log ların içinde ilgili hata mesajını görebilirsiniz.

Hedef: wperl mrtg --logging=eventlog mrtg.cfg

Dizin: c:\mrtg-2.10.13\bin

Eğer startup (başlangıç) dizinine yukarıdaki bilgileri kısayol yapıp koyarsanız bilgisayarınız her açılışında otomatik olarak hazırladığınız scripti çalıştıracaktır. Bu sayede mrtg programı kesintisiz bir şekilde her 5 dakikada bir bilgisayarınızda çalışacak ve istediğiniz bilgileri toplayacaktır.

Tabii mrtg'yi bilgisayarınızda devamlı çalıştırmak için sadece bu yöntemi kullanmak zorunda değilsiniz. Bazı yardımcı yazılımlar ile bu işlemi bilgisayarınızda çalışan bir servis gibi düzenleyip kullanmanızda mümkün. Bir sonraki bölümde bu işlemin nasıl yapılacağı konusuna değinicez.

Aşağıda, Cisco Cat 5000 üzerindeki 3, 5, 10 ve 24 nolu interfacelerdeki trafik ölçülüp router'ın CPU yükünü kontrol eden örnek bir mrtg.cfg dosyası bulunuyor. Bu örnekte kullanacağınız OID'yi biliyorsanız nasıl SNMP ile cihazları kontrol edebileceğinizi görebilirsiniz. Bu dosyayı inceleyerek config. dosyaları hakkında daha net bir bilgiye sahip olabilirsiniz.

WorkDir: D:\InetPub\wwwroot\MRTG

```
 ###################################################################### ########
# Description: LCP SUWGB
# Contact: Seyhan Tekelioglu
# System Name: LC-Bridge
 #..................................................... .....
Target[10.10.10.1.1]: 3:public@10.10.10.1
MaxBytes[10.10.10.1.1]: 1250000
Title[10.10.10.1.1]: LC-Bridge (sample-device): ether0
PageTop[10.10.10.1.1]: <H1>Traffic Analysis for ether0</H1>
 <TABLE>
<TR><TD>System:</TD><TD>LC-Bridge inAndover</TD></TR>
<TR><TD>Maintainer:</TD><TD>Seyhan Tekelioglu</TD></TR>
 <TR><TD>Interface:</TD><TD>ether0(3) </TD></TR>
 <TR><TD>IP:</TD><TD>sample-device(10 .10.10.1)</TD></TR>
<TR><TD>Max Speed:</TD>
<TD>1250.0 kBytes/s (ethernetCsmacd)</TD></TR>
</TABLE>
 #-------------------------------------------------------- ----
Target[10.10.10.1.2]: 5:public@10.10.10.1
MaxBytes[10.10.10.1.2]: 1250000
Title[10.10.10.1.2]: LC-Bridge (): ulink0
PageTop[10.10.10.1.2]: <H1>Traffic Analysis for ulink0</H1>
 <TABLE>
 <TR><TD>System:</TD><TD>LC-Bridge inAndover</TD></TR>
 <TR><TD>Maintainer:</TD><TD>Seyhan Tekelioglu</TD></TR>
  <TR><TD>Interface:</TD><TD>ulink0(5) </TD></TR>
    <TR><TD>IP:</TD><TD>()</TD>< ; ; ;/TR>
 <TR><TD>Max Speed:</TD>
```

```
 <TD>1250.0 kBytes/s (ethernetCsmacd)</TD></TR>
 </TABLE>
 #-------------------------------------------------------------- ----
Target[10.10.10.1.1]: 10:public@10.10.10.1
MaxBytes[10.10.10.1.1]: 1250000
Title[10.10.10.1.1]: LC-Bridge (sample-device): ether0
PageTop[10.10.10.1.1]: <H1>Traffic Analysis for ether0</H1>
 <TABLE>
 <TR><TD>System:</TD><TD>LC-Bridge inAndover</TD></TR>
 <TR><TD>Maintainer:</TD><TD>Seyhan Tekelioglu</TD></TR>
  <TR><TD>Interface:</TD><TD>ether0(10 )</TD></TR>
  <TR><TD>IP:</TD><TD>sample-device(10 .10.10.1)</TD></TR>
 <TR><TD>Max Speed:</TD>
 <TD>1250.0 kBytes/s (ethernetCsmacd)</TD></TR>
 </TABLE>
 #-------------------------------------------------------------- ----
Target[10.10.10.1.2]: 24:public@10.10.10.1
MaxBytes[10.10.10.1.2]: 1250000
Title[10.10.10.1.2]: LC-Bridge (): ulink0
PageTop[10.10.10.1.2]: <H1>Traffic Analysis for ulink0</H1>
 <TABLE>
 <TR><TD>System:</TD><TD>LC-Bridge inAndover</TD></TR>
 <TR><TD>Maintainer:</TD><TD>Seyhan Tekelioglu</TD></TR>
  <TR><TD>Interface:</TD><TD>ulink0(24 )</TD></TR>
    <TR><TD>IP:</TD><TD>()</TD>< ; ; ;/TR>
 <TR><TD>Max Speed:</TD>
 <TD>1250.0 kBytes/s (ethernetCsmacd)</TD></TR>
 </TABLE>
 #-------------------------------------------------------------- ----
# Router CPU load %
Target[cpu.1] :1.3.6.1.4.1.9.2.1.58.0&1.3.6.1.4.1.9.2.1.58.0:public@10 .10.10.1
RouterUptime[cpu.1]: public@10.10.10.1
MaxBytes[cpu.1]: 100
Title[cpu.1]: CPU LOAD
PageTop[cpu.1]: <H1>CPU Load %</H1>
Unscaled[cpu.1]: ymwd
ShortLegend[cpu.1]: %
XSize[cpu.1]: 380
YSize[cpu.1]: 100
YLegend[cpu.1]: CPU Utilization
Legend1[cpu.1]: CPU Utilization in % (Load)
Legend2[cpu.1]: CPU Utilization in % (Load)
Legend3[cpu.1]:
Legend4[cpu.1]:
LegendI[cpu.1]:
LegendO[cpu.1]:  Usage
Options[cpu.1]: gauge
```

Bölüm 2 : MRTG'nin Servis Olarak Çalıştırılması

Giriş :

Mrtg network trafiğini kontrol etmek için çok kullanışlı bir program. Bunu daha da kolay bir hale sokmak için kullanabileceğimiz yardımcı yazılımlar mevcut. Bu yazılımlardan bir tanesi de mrtg'yi bizim için Nttabanlı makinelerde servis haline getiren **FireDaemon**

yazılımıdır. Bu yazılım sayesinde belirli aralıklarla mrtg scriptimiz çalıştırılır ve trafik grafiğini öıkartmamıza yardımcı olur.

FireDaemon yazılımı NT/2K/XP/2K3 işletim sistemleri altında servis olarak sorunsuz bir şekilde çalışabilmektedir. Yalnız size tavsiyem bu programı kullanmadan önce mrtg'yi manuel olarak çalıştırıp her şeyin yolunda olduğundan emin olmanız ve son işlem olarakta FireDaemon ile bunu otomasyona sokmanız olacaktır.

Kuruluma başlamadan önce mrtg kurulu serverda tüm güvenlik patchlerinin ve son update'lerin geçili olduğundan emin olun. Windows XP Home veya Professional ve Windows Server 2003 (NT 5.1 ve 5.2) işletim sistemlerinden birini kullanıyorsanız Windows Update'i çalıştırarak tüm kritik update'leri (Critical Updates) geçin. Windows 2000 (NT 5.0) Professional, Server veya Advanced Server için Service Pack 3 (veya üstü) kurulu olmalı, Internet Explorer 6.0 versiyonu yüklü olmalı, yine bu işletim sistemleri içinde Windows Update çalıştırarak tüm kritik update'leri (Critical Updates) geçin. Windows NT 4.0 Workstation veya Server için Service Pack 6a plus geçili olmalı ve Internet Explorer 6.0 versiyonunu yüklemelisiniz.

Mrtg Konfigürasyonu :

Bölüm 1'de anlatılan konfigürasyon dosyası üzerinde yapacağımız değişikliklerle FireDaemon'u nasıl aktif edileceğine bir göz atalım.

Standart konfigürasyon dosyamızın en tepesine iki yeni satır eklenir. Bunlardan ilki mrtg'nin servis olarak çalışacağını ve ikincisi işlemimizin 5 dakikada bir tekrarlanacağını gösteren satırlardır.

RunAsDaemon: yes
Interval: 5

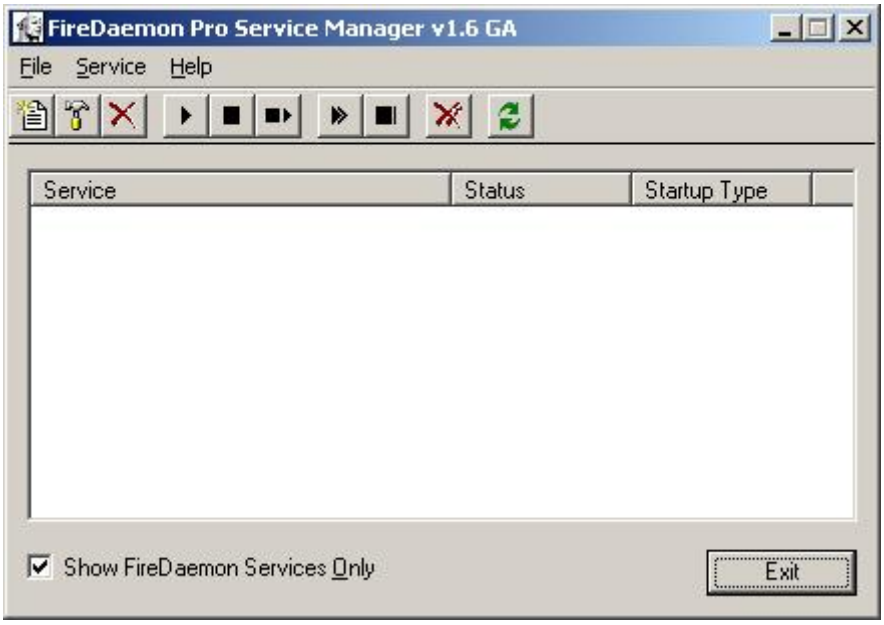
WorkDir: D:\InetPub\wwwroot\MRTG

#######
 # Description: LCP SUWGB
 # Contact: Seyhan Tekelioglu
 # System Name: LC-Bridge
 # Location: Here
#..... .....
Target[10.10.10.1.1]: 3:public@10.10.10.1
MaxBytes[10.10.10.1.1]: 1250000

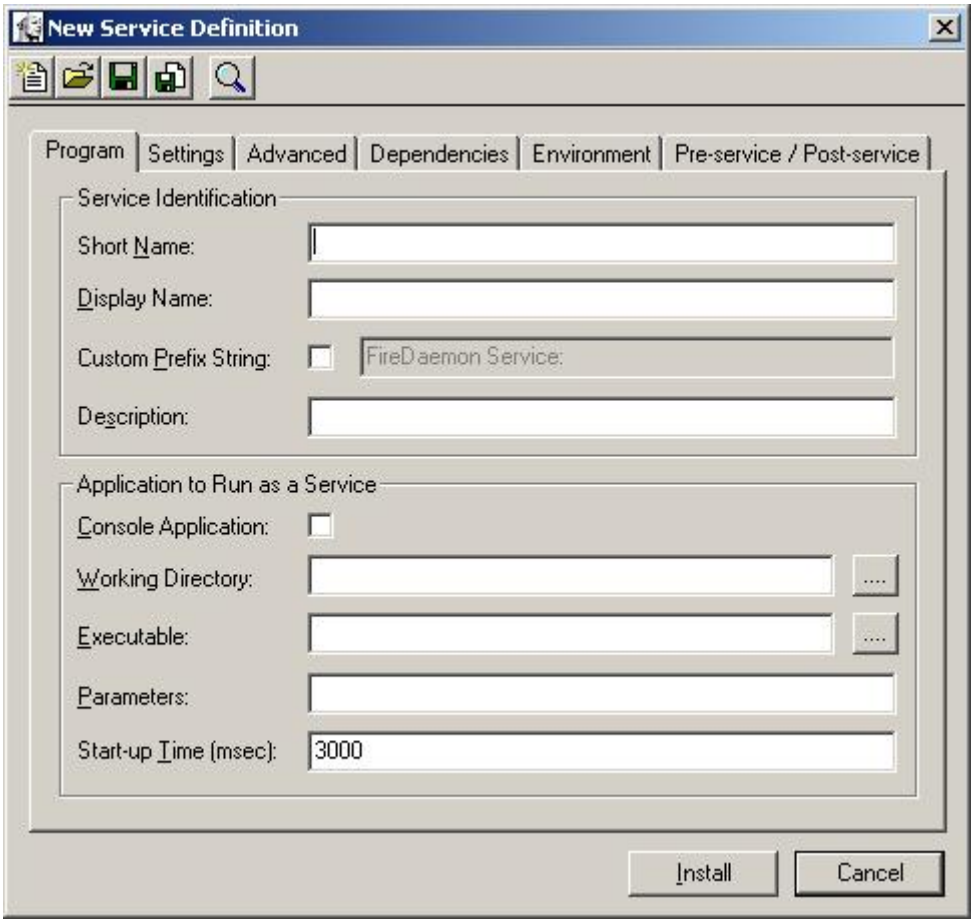
…..

FireDaemon Konfigürasyonu :

FireDaemon programını makinenize kurduktan sonra ilk yapmamız gereken bir servis olarak çalışır duruma getirmektir. Bunu yapabilmek için *Start* > *Programs* menüsünden FireDameon Service Manager'I kullanacağız.

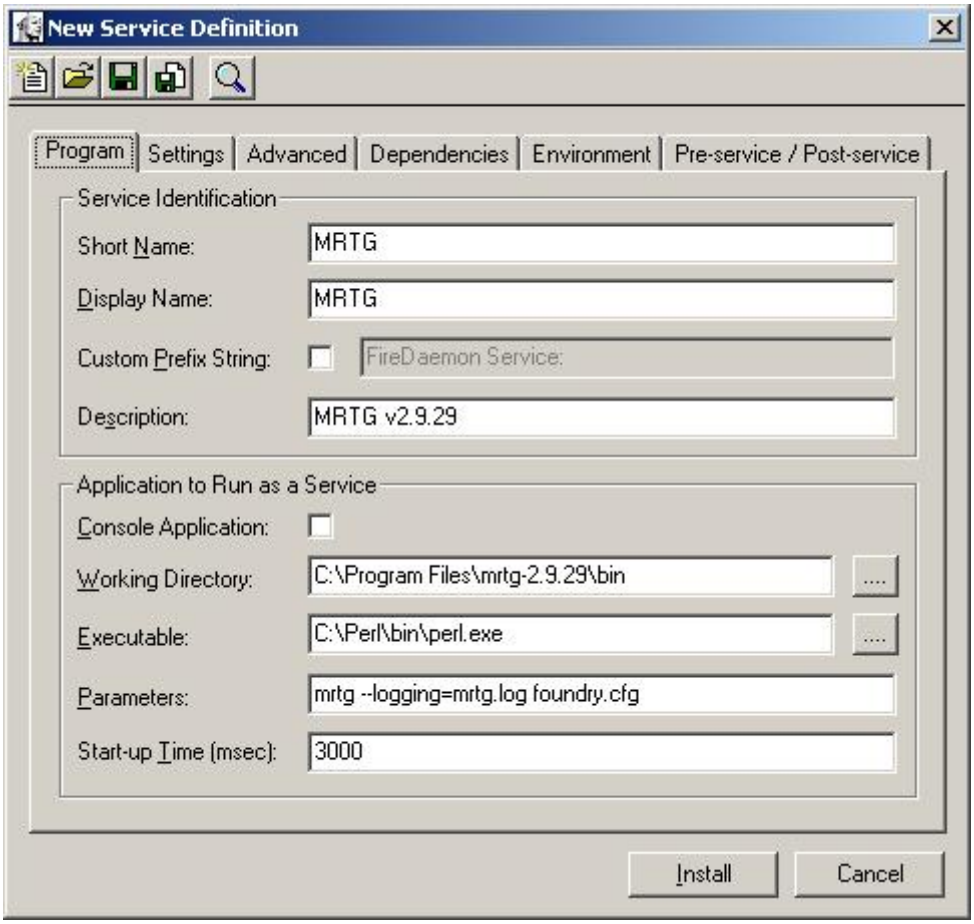


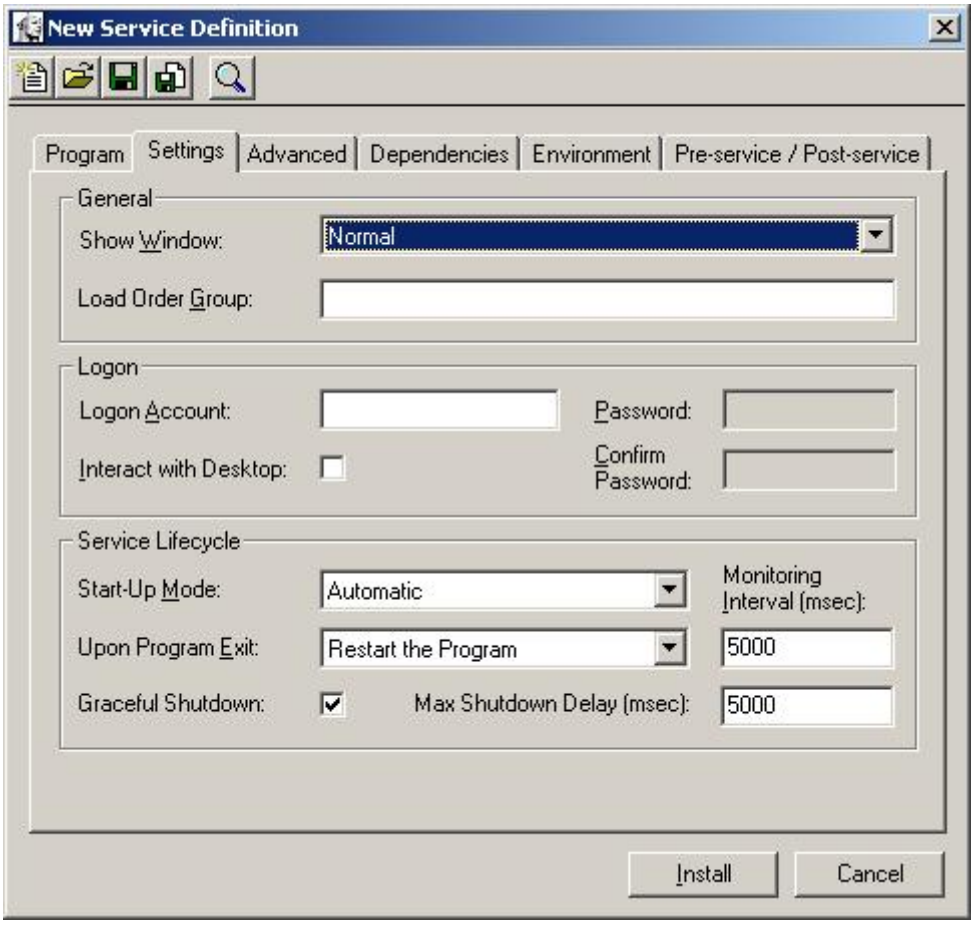
Şimdi yeni bir tanımlama yapacağız bunun için *Create A New Service Definition* düğmesine basın yada kısayol olarak *CTRL + N* tuş kombinasyonunu kullanabilirsiniz.



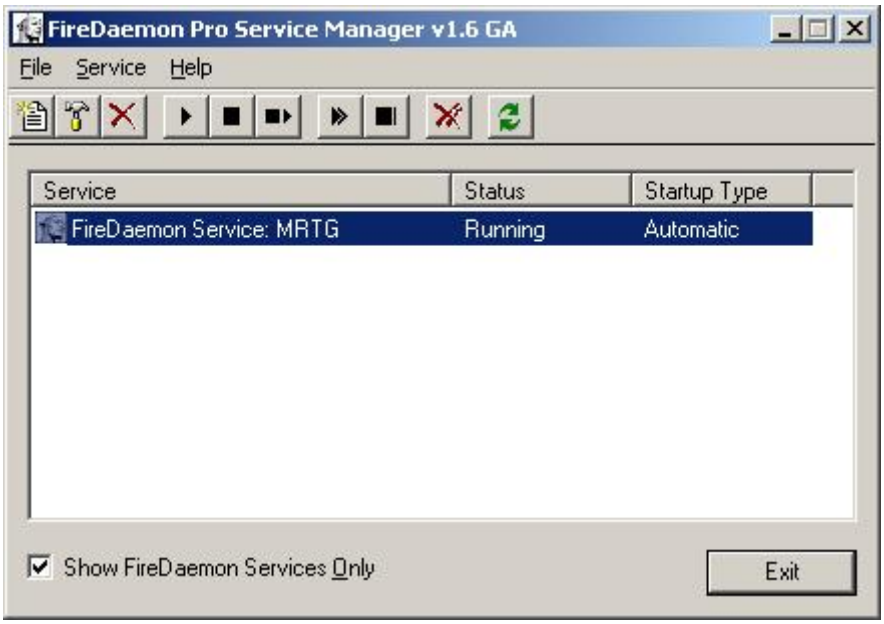
Karşımıza çıkan bu ekranı aşağıdaki şekilde doldurarak konfigürasyonun bu aşamasını tamamlayacağız. Tabi program yolu ve config. dosyası adınızı farklı verdiyseniz onları kendi ayarlarınıza göre değiştirmelisiniz. Burada Bölüm 1'de oluşturulan conf. dosyasına göre

düzenleme yapıyoruz. Menüler arasında hareket için *TAB* vyea *SHIFT* + *TAB* tuşlarını kullanabilirsiniz.





Buraya kadar yaptığımız işlemler tamam. Şimdi servisi kurmak için *Install* tuşuna basın. Servis sorunsuz olarak kurulmalı ve servisler altında görünmeli. Bunu Task Manager'dan kontrol edebilirsiniz. Ayrıca Event Log'lara bakarak FireDameon'un vereceği olası hata veya uyarı mesajlarını görmeniz mümkün.



Normal FireDaemon programı ücretsiz olarak indirilebiliyor fakat aynı makine içinde birden fazla mrtg çalıştırmak istiyorsanız FireDaemon Pro'yu satın almalısınız. FireDaemon Pro'da her bir mrtg için ayrı servis adı vererek birden çok mrtg çalıştırabiliyorsunuz.