### RSYSLOG

# İÇİNDEKİLER

1.Syslog nedir?

2.Rsyslog nedir?

3.Rsyslog Kurulumu

3.1.Centos Üzerinde Rsyslog Kurulumu

3.2. Rsyslog’ un Test edilmesi

3.3. Rsyslog’un Debug Edilmesi

4.Rsyslog Yapılandırma İşlemleri

5. Centos’tan Log Forwarding

5.1.Log Sunucularındaki İşlemler

5.1.1. Logları Text Dosyalarında Tutmak

6 .Centosun Yapılanırılması

6.1 . Üretilen Tüm İletilerin Log Sunucusuna Gönderilmesi

6.2. Sadece Belirli Fasilitelerin Log Sunucusuna Gönderilmesi

## 1.Syslog Nedir ?

Syslog, bildiğiniz gibi \*nix sistemlerdeki çeşitli kaynaklar ya da uygulamalarca üretilen

log’ları (ileti) işlemekle görevli bir uygulamadır. Syslogd isimli bir daemon olarak çalışan

syslog, üretilen iletilerin ne şekilde değerlendirileceğini belirler. Örneğin, üzerinde de bir

smtp sunucusu çalışan \*nix sisteminizde, klasik olarak smtp daemon’ı, mail aktivitesi ile

ilgili logları syslog’a gönderir, syslog bu logları alıp, bir dosyaya yazar ya da belirli bir e-mail

adresine postalar ve ya direk olarak konsola basar. Sonuç olarak siz, herhangi bir kaynaktan

gelen logların ne şekilde değerlendirilmesini istediğinizi syslog’a söylersiniz ve syslog bu

istekleri yerine getirir.

Syslog’un ön tanımlı ayarlarına göre hemen hertür \*nix sistemde, ilgili kaynaklar (fasilite)

tarafından üretilen ve syslog tarafından düzenlenen loglar /var/log dizini içerisinde ayrı

dosyalar halinde bulunur. Bu şekilde sunucunuzda herhangi bir sorun olduğu zaman ilk

başvurduğumuz kaynaklar olan logların düzenli bir şekilde tutulması sağlanmaktadır.

Syslog üzerinde çalıştığı sistemin loglarını işlediği gibi uzaktaki bir sistemden gönderilen

logları da alıp işleme yetisine sahiptir. Bu iş için syslog sunucunuzun network özelliğini

devreye almak ve bir iki küçük ayarlama yapmak yeterli olacaktır . Böylece, syslog tcp ya da

udp 514. portu dinleyerek bu porta ulaşan log çıktılarını alabilir ve istediğiniz doğrultuda

işleyebilir. Zaten, bu yazının konusu da bu.

Ancak yazının başlığından da anlaşılacağı gibi ben log işlemek için syslog yerine rsyslog

kullanmaktayım. Şimdi rsyslog’un ne olduğu ve neden rsyslog kullandığını konusunda bilgi edinelim.

## 2.Rsyslog Nedir ?

Rsyslog, syslogd’nin geliştirilmiş halidir. Çoğunu syslogd ile de yapabileceğiniz gibi rsyslog

kullanarak, logları MySQL, postgreSQL, Oracle vs gibi database’lere yazdırabilirsiniz. Alınan

logların formatları ile istediğiniz gibi oynayabilirsiniz. Logları encrypt edebilirsiniz. Text

dosyalarını syslog formatına sokabilirsiniz vs. Örnekleri çoğaltmak da mümkündür.

Rsyslog’un yetenekleri ile ilgili tam bir listeye için şu adresten ulaşabilirsiniz:

http://www.rsyslog.com/module-Static\_Docs-view-f-features.html.phtml

Sunduğu özelliklerin yanı sıra rsyslog’a sempatimin bir diğer nedeni de rsyslog ve

phplogcon\* ile uğraşırken, hem rsyslog baş geliştiricisi Rainer Gerhards’ın hem de phplogcon

geliştiricisi Andre Lorbach’ın sorduğum sorular karşısında gösterdikleri yardımseverliktir.

Sonuç olarak rsyslog ile ilgili herhangi bir sorunla karşılaşınca direk olarak geliştiricisine

ulaşabilmek ve kendisinin epey yardım sever birisi olması gayet güzel bir durum.

(\*) Phplogcon, rsyslog ile birlikte kullanılabilen web arayüzüdür. Sunucu loglarının web

tabanlı olarak online monitor edilebilmesi için oldukça kullanışlı bir yazılımdır. Bir sonraki

yazımda konu PhpLogcon kurulumuna değineceğim.

Syslog ve Rsyslog ile ilgili temel bilgilere değindikten sonra, rsyslog kurulum notlarına

geçebiliriz.

## 3.Rsyslog Kurulumu

Eğer Fedora ya da Debian Lenny kullanıyorsanız, rsyslog kullanmak için herhangi bir

kurulum yapmanıza gerek kalmıyor. Çünkü, rsyslog bu iki dağıtımda ön tanımlı syslog

daemon’ı olarak geliyor. Ancak, rsyslog’un iletileri bir database’de tutmasını istemeniz

durumunda db desteği sunan rsyslog paketlerini ayrıca kurmanız gerekmektedir. Örnel olarak,

Rrsyslog’a MySQL desteği kazandırmak için rsyslog-mysql kurulmalıdır. Şimdi bu işlemi

yapalım.

## 3.1.Centos Üzerinde Rsyslog Kurulumu

Şimdi ise [CentOS](https://www.syslogs.org/tag/centos/) bir sistemde, rsyslog kurulumu ve syslog’un rsyslog ile değiştirilmesi işleminin nasıl yapılacağından bahsetmek istiyorum.

[CentOS](https://www.syslogs.org/tag/centos/) üzerine rsyslog kurulumu ve yapılandırmasını bir kaç adımda halletmek mümkün. İlgili yazılımın rpm dosyaları, [CentOS](https://www.syslogs.org/tag/centos/) paket depolarında bulunduğundan dolayı, kurulumu yum ile yapmak mümkün. Kurulum sonucunda, sistem syslogd’nin ayarları ile çalışmak üzere ayarlanmış oluyor. Aşağıdaki adımları takip ederek kurulumu gerçekleştirebilirsiniz.

## Kurulum

rsyslog paketini yum kullanarak her zamanki gibi kuruyoruz.

#yum install rsyslog

Kurulumdan sonra yapılandırma işlemlerine geçebiliriz.

## Yapılandırma

sistemde syslog ve rsyslog olmak üzere iki adet log daemon’ı yüklü duruma geliyor. Chkconfig –list ile kontrol edebilirsiniz:

# chkconfig --list |grep syslog

Çıktı şu şekilde olacaktır:

rsyslog 0:off 1:off 2:off 3:off 4:off 5:off 6:off

syslog 0:off 1:off 2:on 3:on 4:on 5:on 6:off

Yukarıdaki çıktıda görüldüğü gibi hem syslog hem de rsyslog sisteme yüklü durumda. Syslog 2,3,4 ve 5. run level’larda otomatik olarak çalıştırılmak üzere ayarlanmış görünüyor. Şimdi biz syslog’u tüm run levellar’da off duruma getirip, rsyslog’u 2,3,4 ve 5 için on durumuna getireceğiz:

# chkconfig --level 2345 syslog off

# chkconfig --level 2345 rsyslog on

Tekrar kontrol ettiğiniz zaman syslog’un devre dışı bırakılıp rsyslog’un on duruma getirildiğini görebilirsiniz. Bu işlem tamam, ancak şu an syslogd sistemde çalışmakta. Bu nedenle, önce syslogd’yi durduruyoruz:

# service syslog stop

Sonra da rsyslog’u start ediyoruz.

# service rsyslog start

Artık rsyslog devrede ve syslog’un görevini almış durumda. ps ile kontrol edelim:

# ps aux |grep rsyslog

Çıktı şuna benzer olacaktır:

root 4557 0.0 0.3 12284 912 ? Sl 12:53 0:00 rsyslogd -m 0

Herşey yolunda görünüyor. Rsyslog, /etc/rsyslog.conf dosyasının içeriğinden kareket ederek logları işleyecektir ve bu dosyanın içeriği orjinal syslog.conf dosyası ile aynı olduğu gibi loglar herzamanki gibi işlenmeye devam edecektir. Birazdan testleri yapacağız ancak önce, rsyslog’un uzak sunuculardan da log alabilmesi için network özelliğini aktif edelim.

/etc/sysconfig/rsyslog dosyasını editleyin:

# vi /etc/sysconfig/rsyslog

Dosya içerisinde aşağıdaki satırı bulun:

SYSLOGD\_OPTIONS="-m 0"

ve -m 0 ibaresinin hemen yanında -r514 parametresini ekleyin:

SYSLOGD\_OPTIONS="-m 0 -r514"

Bu şekilde rsyslog’un network desteği aktif olacak ve udp 514 portunu dinlemeye başlayacaktır. Ancak değişikliklerin devreye girmesi için rsyslog’u restart etmek gerekiyor.

# service rsyslog restart

Herşey yolunda gittiyse, şimdi rsyslog’un çalışıp çalışmadığını kontrol edelim.

### 3.2.Rsyslogun Test Edilmesi

Test için logger komutundan yararlanılıp bir log üretilebilir:

# logger "Bu log'un, /var/log/messages dosyasına yazılması gerekir."

Komutun sonucu olarak, üretilen log, /var/log/messages dosyasına yazılacaktır. tail ile bakalım:

# tail /var/log/messages

Çıktıda aşağıdak gibi bir satır görmeniz gerekir.

Aug 31 14:03:20 test-[centos](https://www.syslogs.org/tag/centos/) root: Bu log'un, /var/log/messages dosyas.na yazılması gerekir.

Bir de rsyslog’u yapılandırırken, network özelliğini devreye almıştık. Dolayısı ile şu an rsyslog’un udp 514. portu dinliyor olması gerekir. Bunu da kontrol etmek için netstat komutundan yararlanabiliriz.

# netstat -an |grep 514

Çıktı şu şekilde olacaktır:

udp 0 0 0.0.0.0:514 0.0.0.0:\*

udp 0 0 :::514 :::

Görüldüğü gibi udp 514 bind edilmiş durumda. Bu şekilde uzak sistemlerden rsyslog’a ileti gönderebilir ve merkezi log sunucusu olarak kullanabilirsiniz. Bu işlemin nasıl yapıldığını, Rsyslog ile Merkezi Log Sunucusu Kurulumu başlıklı yazıda bulabilirsiniz.

Son olarak, herhangi bir problem durumunda rsyslog’un debug edilmesi işlemine değinmek istiyorum.

### 3.3.Rsyslog’un Debug Edilmesi

Önce rsyslog’u stop edin:

# service rsyslog stop

Sonrasında simdi rsyslog’u komut satırından maneul olarak debug parametreri ile başlatıyoruz.:

# rsyslogd -m 0 -r514 -d

Bu şekilde rsyslog ile ilgili ne olup bittiğini ekrandan takip edebilirsiniz.

## 4.Rsyslog Yapılandırma İşlemleri

Öncelikle, sistemdeki rsyslog’u merkezi log sunucusu olarak kullanabilmek için network

desteğinin devrede olması gerekmektedir. Bu destek, /etc/rsyslog.conf dosyasında

aktifleştirilmelidir.

Şimdi, rsyslog.conf dosyasını editleyelim.

Komut

# /etc/rsyslog.conf

# /etc/rsyslog.conf

Dosya içerisinde network desteği ile ilgili satırlar aşağıda görüldüğü gibi ön tanımlı olarak

mevcuttur. Ancak # ile comment out edilmiş ve devre dışı bırakılmışlardır. Networking

desteğini aktif etmek için açıklama satırları hariç diğer satırların başındaki # işaretini

kaldırmalı ve uncomment etmelisiniz.

Yani şu şekilde görünmelidir.

Çıktı

# provides UDP syslog reception

$Modload imudp

$UDPServerRun 514

# provides TCP syslog reception

$Modload imtcp

$InputTCPServerRun 514

# provides UDP syslog reception

$ModLoad imudp

$UDPServerRun 514

# provides TCP syslog reception

$ModLoad imtcp

$InputTCPServerRun 514

Artık dosyayı kaydedip çıkabilirsiniz. Şimdi değişikliklerin aktif olması için rsyslog’u

yeniden başlatıyoruz:

Komut

# /etc/init.d/rsyslog restart

# /etc/init.d/rsyslog restart

Rsyslog restart edildikten sonra, hem tcp hem de udp 514. portlar rsyslog tarafından

dinlenmeye başlanmış olmalıdır. Kontrol etmek için netstat komutundan yararlanalım.

Komut

# netstat -an ­|grep 514

# netstat -an |grep 514

Çıktı şu şekilde olmalıdır:

Çıktı

C:\Users\acer\Desktop\gv.png

tcp 0 0 0.0.0.0:514 0.0.0.0:\* LISTEN

tcp6 0 0 :::514 :::\* LISTEN

udp 0 0 0.0.0.0:514 0.0.0.0:\*

udp6 0 0 :::514 :::\*

tcp 0 0 0.0.0.0:514 0.0.0.0:\* LISTEN

tcp6 0 0 :::514 :::\* LISTEN

udp 0 0 0.0.0.0:514 0.0.0.0:\*

udp6 0 0 :::514 :::\*

Görüldüğü üzere ilgili portlar bind edilmiş durumdalar.

Şu anda, rsyslog temel olarak ayarlanmış durumda.

## 5.Centos’dan Log Forwarding

Centos sistemlerde, ön tanımlı olarak syslog kullanılmaktadır. Syslog’un conf dosyası ise

/etc/syslog.conf’tur.

Bir Centos’dan uzaktaki bir log sunucusuna ileti göndermek için tercih edebileceğiniz iki

yol bulunmaktadır. Bunlardan birisi, syslog’un ürettiği tüm iletileri uzaktaki log sunucusuna

göndermektir. Diğeri ise, sadece belirli fasilitelerce üretilen logların sunucuya iletilmesidir.

Bu durumda tüm loglar yerine örneğin sadece auth. loglarını gönderebilirsiniz.

Ben her iki yönteme de değineceğim, siz sisteminizi ihtiyacınız olan şekilde

yapılandırabilirsiniz.

Üretilen tüm iletilerin log sunucusuna gönderilmesi için aşağıdaki adımları uygulamanız

yeterlidir.

/etc/syslog.conf dosyanızı editleyin.

Komut

vi /etc/syslog.conf

vi /etc/syslog.conf

Dosyanın en üstüne aşağıdakine benzer bir satır ekleyin. (Satırın en üste eklenmesi

önemlidir.) Benim rsyslog sunucumun ip adresi **46.221.172.136 satır** şu şekilde:

Çıktı

\*.\* @192.168.12.242

(\*.\*) @**46.221.172.136**

Bu satırda, tüm logların ip adresli sisteme yollanmasını söylüyoruz. Ip

adresinin başındaki @ işareti logların UDP protokolü ile gönderilmesini söylemektedir. @@

şeklinde iki at işareti koyarsanız iletiler TCP üzerinden gönderilirler. Çok fazla log trafiği

olan sistemler için tcp yerine udp kullanmak tercih edilir.)

Artık Centos’da üretilen tüm loglar, rsyslog sunucusuna gönderilecektir.

Diğer alternatif ise sadece belirli fasilitelerce üretilen iletilerin, log sunucusuna

gönderilmesidir.

Tüm loglar yerine örneğin sadece auth ya da mail loglarını log sunucusuna

göndermek isteyebilirsiniz. Bu durumda, syslog.conf dosyasında yukarıda olduğu gibi \*.\*

kullanmak yerine sadece istediğiniz fasiliteyi belirtebilirsiniz.

Örnek olarak sadece auth ile ilgili logların gönderilmesi için syslog.conf dosyasının en

tepesine şu şekilde bir satır eklemek yeterli olacaktır.

Çıktı

Auth.info;authpriv.info @**46.221.172.136**

auth.info;authpriv.info @192.168.12.242

Böylece, sadece login vs. işlemleri ile ilgili loglar iletilecektir.

Son olarak değişikliklerin geçerli olması için syslog servisini yeniden başlatın

Şimdi değişikliklerin aktif olması için syslog’u restart ediyoruz.

Komut

/etc/rc.d/syslogd restart

/etc/rc.d/syslogd restart

Evet, normal şartlarda herşey düzgün çalışıyor olmalıdır. Şimdi test edelim.

## Log Sunucusunun Test Edilmesi

Test işlemi için logger komutundan yararlanılabilir. Ben, Centos üzerinde tüm logların

rsyslog sunucusuna gönderilemesi için ayarlama yaptım. Dolayısı ile şimdi Centos ‘da

logger komutu ile bir notice mesaji göndereceğim.

Komut

#logger “Bu mesaji rsyslog sunucusunun ilgili log dosyasına yada db tablosunda gormemiz gerekir.”

# logger "Bu mesaji rsyslog sunucusunun ilgili log dosyasinda ya da db

tablosunda gormeniz gerekir."

Üretilen bu log, Centos’un kendi üzerinde messages dosyasına yazılacaktır.

Eğer siz, sadece belirli fasilitelere ait logları gönderiyorsanız, bu durumda ilgili fasiliteler için

bir ileti oluşturup kontrol etmelisiniz.

Testlerinizi yaptınız ve iletilerin, log sunucusundaki ilgili dosyalara yazılmadığını gördünüz.

Bu problemin nedenini anlamanın en güzel yolu, rsyslog’u debug mod’da çalıştırmaktır.

Debug özelliğini devreye almak için şu işlemleri yapabilirsiniz.

Önce, rsyslog servisini durdurun:

Komut

# /etc/init.d/rsyslog restart

# /etc/init.d/rsyslog restart

Sonrasında da şu komutu verin:

Çıktı

/usr/sbin/rsyslogd –c3 -d

rsyslog debug modda çalışınca, uzaktaki sistemden tekrar log göndermeyi deneyebilir, debug

çıktılarından problemi tespit edebilirsiniz.

Centos sistemlerden log forwarding ile ilgili genel geçer yapılandırma işlemleri bu şekildedir.

## 5.1.Log Sunucusundaki İşlemler

Bu kısımda ayrı ayrı hem logları text tabanlı dosyalara yazdırmaktan, hem de MySQL

DB’sine yazma işleminden bahsedeceğim.

## 5.1.1.Logları Text Dosyalarında Tutmak

Gene tüm logları, tek bir dosyaya ya da fasilitelerine göre birden fazla log dosyasına

yazdırmanız münkün.

Test için kullandığım CentOS’un hostname’i centtest, bu sistemden gelen “tüm” logları

/var/log/centtest.log dosyasına yazdırmak için rsyslog.conf dosyasına şu satırları ekliyorum:

Çıktı

+centtest

\*.\* var/log/centtest.log

+centtest

\*.\* /var/log/centtest.log

Logları tek dosyaya yazdırmak için bu giriş yeterli.

Eğer fasilitelere göre ayrıştırmak isterseniz, örneğin, cron ile ilgili logları, /var/log/centtest-

cron.log dosyasına yazdırmak için rsyslog.conf dosyasına şu satırı ekleyebilirsiniz.

Çıktı

+centtest

Cron.\* /var/log/centtest-cron.log

+centtest

cron.\* /var/log/centtest-cron.log

Örnekleri kendi isteklerinize göre çoğaltabilirsiniz.

Şimdi **46.221.172.136**  ip adresli centtest makinası için rsyslog sunucusunun /etc/hosts

dosyasına aşağıdaki satırı girelim.

Çıktı

**46.221.172.136 centtest**

192.168.12.234 centtest

Sonra da rsyslog’u restart edelim.

Komut

/etc/init.d/rsyslog restart

İletileri text tabanlı dosyalara yazdırmak için gerekli Rsyslog yapılandırma bu şekildedir.

/etc/init.d/rsyslog restart

İletileri, text tabanlı dosyalara yazdırmak için gerekli Rsyslog yapılandırması bundan ibaret.

## 6.Centosun Yapılandırılması

Burada da aynı şekilde rsyslog sunucusuna tüm logları gönderebileceğiniz gibi sadece

seçtiğiniz fasilitelere ait logların gönderilmesini sağlayabilirsiniz.

## 6.1.Üretilen tüm iletilerin log sunucusuna gönderilmesi

Bunun için /etc/syslog.conf dosyasının içine şu satırı eklemek yeterli.

Çıktı

\*.\* @**46.221.172.136**

\*.\* @192.168.12.242

Böylece tüm loglar 192.168.12.242 ip’li rsyslog sunucusuna udp üzerinden forward

edilecektir.

## 6.2.Sadece belirli fasilitelerce üretilen iletilerin log sunucusuna gönderilmesi

Örneğin sadece cron ile ilgili logları forward etmek için şu /etc/syslog.conf dosyasına şu

şekilde bir satır girebilirsiniz.

Çıktı

Cron.\* @**46.221.172.136**

cron.\* @192.168.12.242

Böylece sadece cron ile ilgili loglar, rsyslog’a iletilecektir.

Gerekli eklemeleri yaptıktan sonra syslog’u restart ediyoruz.

Komut

# service syslog restart

# service syslog restart

Herşey yolunda gittiyse, loglar forward edilecektir. Test etmek için gene logger komutundan

yararlanabilirsiniz.