



# Zaman Damgası - Web Logları

Teknik Destek Grubu  
ODTÜ BİDB

16 Mart 2009



# Gündem

- Yönetmelik
- Akış şeması
- Log çevirme
  - rotatelog
  - logrotate
- Veri tabanına verileri aktarma



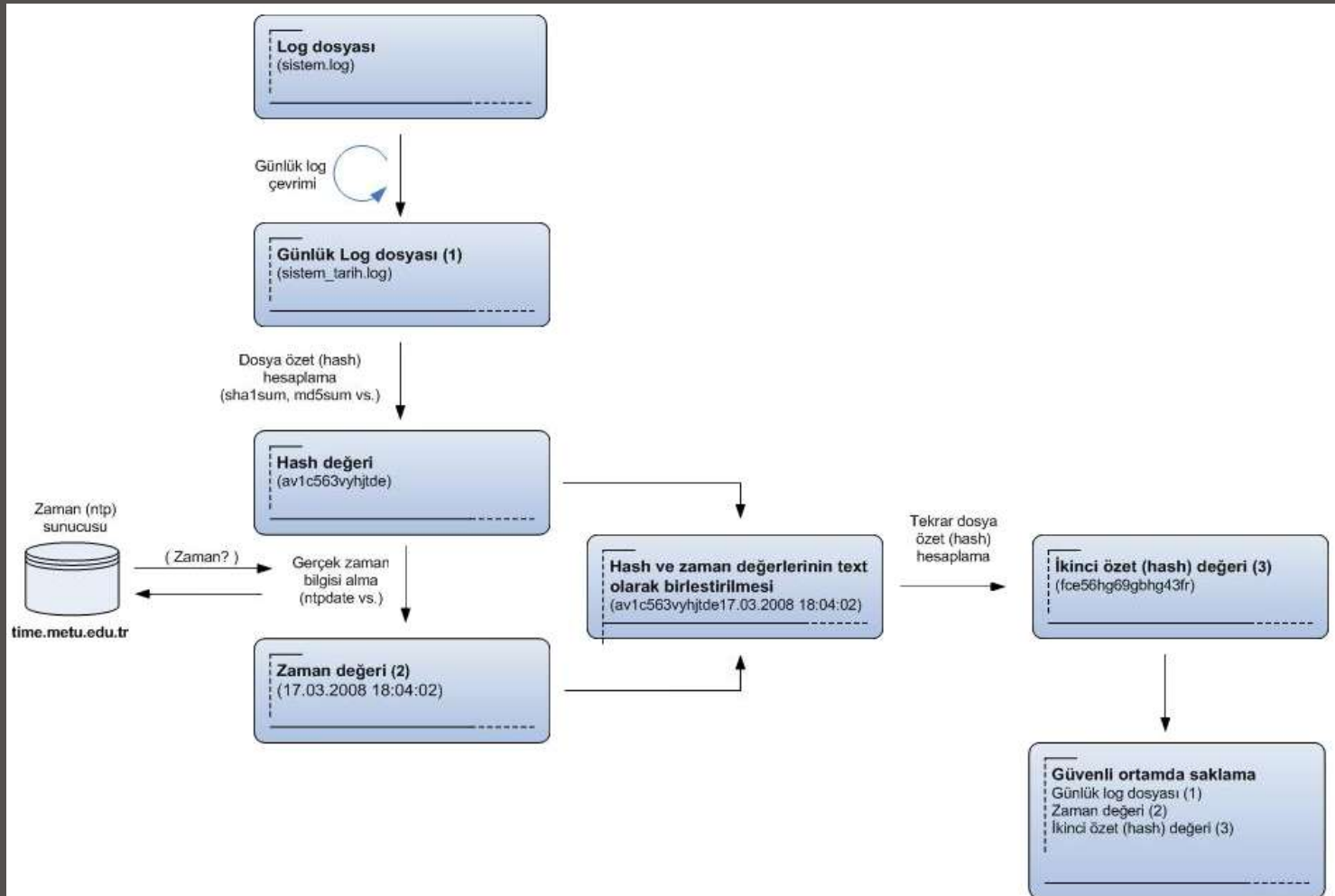
## Yönetmelik

- İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul Ve Esaslar Hakkında Yönetmelik, 30 Kasım 2007 tarih ve 26716 sayılı Resmi Gazete.

“Yer sağlayıcı trafik bilgisini altı ay saklamakla, bu bilgilerin doğruluğunu, bütünlüğünü oluşturan verilerin dosya bütünlük değerlerini zaman damgası ile birlikte saklamak ve gizliliğini temin etmekle yükümlüdürler.”



# Akış Şeması



# Log çevirme

- rotatelog

- apache web sunucusu programı

- ```
#ErrorLog logs/error_log
```

- ```
ErrorLog "|/usr/local/apache2/bin/rotatelogs  
/usr/local/apache2/logs/error_log.%Y-%m-%d 86400 120"
```

- ```
#CustomLog logs/access_log common
```

- ```
CustomLog "|/usr/local/apache2/bin/rotatelogs  
/usr/local/apache2/logs/access_log.%Y-%m-%d 86400 120"  
common
```

## Log çevirme

```
CustomLog "|/usr/local/apache2/bin/rotatelogs  
/usr/local/apache2/logs/access_log.%Y-%m-%d 86400 120"  
common
```

- access\_log.%Y-%m-%d dosya biçimi  
access\_log.2009-03-01 bkz. date
- 1 gün = 8640,120 GMT'ye göre kaç dakika  
öndeyiz. Sistem saati ve zaman dilimi ile  
ilintili.
- Apache Module mod\_log\_config



## Log çevirme

- logrotate (unix aracı)
  - /etc/logrotate.conf
  - /etc/logrotate.d/PROGRAM\_ISMI
- man logrotate

## VT'ye giriş

```
#!/bin/bash
```

```
LOGDIZINI=/usr/local/apache2/logs/Access_Log/  
DAY=1
```

```
HOSTNAME=`hostname`  
DB_HOSTNAME='vt_sunucu_ismi'
```

```
for i in `find $LOGDIZINI -daystart -mtime $DAY -a \<\  
    -type f -a -name "[0-9]"`  
do  
    MD5SONUCU=`md5sum $i | cut -f1 -d" "`  
    DATE=`date`  
    DOSYA=`echo $i|cut -f 7- -d"/"`  
    psql -h $DB_HOSTNAME -U username -c "INSERT INTO \<\  
        VALUES('$DOSYA', '$MD5SONUCU', '$HOSTNAME', \<\  
        '$DATE')"
```

```
log_db  
done
```



## VT görüntüsü

```
log_db=# \d web_logs
```

```
Table "public.web_logs"
```

Column	Type	Modifiers
file_name	character varying(256)	not null
md5sum	character varying(45)	not null
machine_name	character varying(25)	not null
md5sumed_at	timestamp with time zone	not null

```
backup.cc.metu.edu.tr.2008-01-15 | b30b4f487e3c7e02b02bc6d990139bd4 | millet | 2008-01-16 00:30:07+02
```

```
www.btm.metu.edu.tr.2008-01-15 | baf67377245f7207230693e9bd46e84f | millet | 2008-01-16 00:30:07+02
```

```
ekders.metu.edu.tr.2008-01-15 | 1b6d8023578d0bf769d1a852e94b6269 | millet | 2008-01-16 00:30:07+02
```

# logları Sıkıştırma

```
#!/bin/bash
```

```
LOGDIZINI=/usr/local/apache2/logs/Access_Log/
```

```
LOGBACKUP=/usr/local/apache/logbackup/
```

```
DAY=4
```

```
ZIPPER=/bin/gzip
```

```
find $LOGDIZINI -daystart -mtime +$DAY -a -type f -a -name \ "[0-9]"  
-exec $ZIPPER {} \;
```

```
find $LOGDIZINI2 -daystart -mtime +$DAY -a -type f -a -name \ "[0-9]"  
-exec $ZIPPER {} \;
```

```
mv $LOGDIZINI/*.gz $LOGBACKUP > /dev/null 2>&1
```



## Özet

- Log çevirme
  - Apache veya logrotate kullanarak.
- Logların md5sum değerleri ile vt'ye girilmesi.
- Logları belirli bir zamandan sonra sıkıştırılır ve başka bir alana taşınır. En az altı ay güvenli bir şekilde saklanmalıdır.
- Bütün işlemlerin zamanlamasını planlayıp betikleri otomatik (ör; crontab) ile çalıştırmak gerekiyor.



Teşekkürler

Sorular?