

Zaman Damgası - Web Logları

Teknik Destek Grubu
ODTÜ BİDB

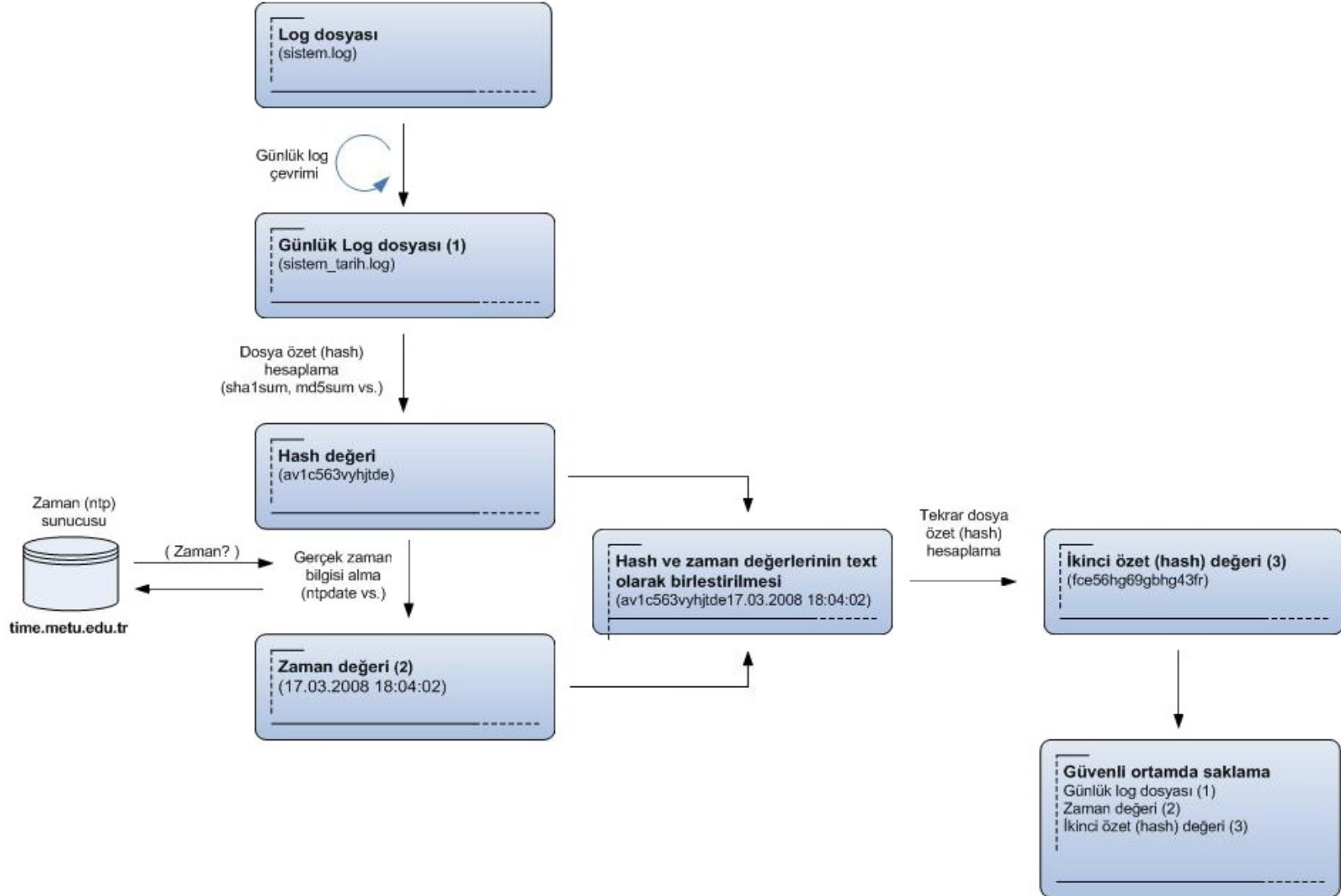
Gündem

- 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/rotatelog /usr/local/apache2/logs/error_log.%Y-%m-%d 86400 120"
```

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

```
CustomLog "|/usr/local/apache2/bin/rotatelog /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.2009-11-16 bkz. date
- 1 gün = 86400 saniye, 120 dakika 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 $DB_HOSTNAME -U vt_kullanici -c "INSERT \<\  
INTO web_logs VALUES('$DOSYA', '$MD5SONUCU', \<\  
'$HOSTNAME' '$DATE')"
```


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 | milet | 2008-01-16 00:30:07+02

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

ekders.metu.edu.tr.2008-01-15 | 1b6d8023578d0bf769d1a852e94b6269 | milet | 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 gir.
- Logları belirli bir zamandan sonra sıkıştır ve başka bir alana taşı. En az altı ay güvenli bir şekilde saklanmalılar.
- Bütün işlemlerin zamanlamasını planlayıp betikleri otomatik (ör; crontab) ile çalıştırmak gerekiyor.