Özgür Yazılım ve Linux Günleri

İstanbul Bilgi Üniversitesi
Dolapdere Kampüsü

2-3 Nisan 2010

İSTANBUL BİLGİ ÜNİVERSİTESİ

LİNUX KULLANICILARI DERNEĞİ TLKD

Nagios ile Ağ/Sunucu İzleme

Kerem ERSOY
e-mail: kerem@sibernet.com.tr
03/Nisan/2010

Nagios®

Nagios Nedir?

- Nagios web-sitesinde yer aldığı haliyle: “Açık Kaynak lisanslaması altında kullanıma sunulan ve kurumsal düzeyde sistemleri, Servisleri ve ağları izleme yazılımıdır.”
- Ancak Nagios sadece izlemekle kalmaz oldukça gelişmiş delegasyon şemalarını da içerecek şekilde, ve değişik ortam ve metodlar kullanarak sistem operatörlerini haberdar eder.
- Örneğin belli bir süre bir e-mail adresine uyarı e-postası göndrip, bu süre içinde sorun çözlmüyorsa sorunu bir üst seviyeye eskale etmek ya da belli günler ve saatler içinde bir kulanıcıya bu saatler dışında başka bir kullanıcıya uyarı mesajı göndermek gibi karmaşık şemalar ile çalışabilir. Ya da e-posta, SMS, Çağrı cihazı gibi değişik araçlar ile uyarı gönderebilir.

Neden Nagios Kullanmalı?

- Açık Kaynaklıdır. (GPL v2 Lisanslı)
- Ölçeklenebilir, yönetilebilir ve güvenlidir.
- Benzeri yazılımlar içerisinde en geniş ve detaylı dökümantasyona sahip yazılımdır.
- Log ve Veritabanı sistemi çok iyi tasarımlıdır.
- Web arabirimi güzel tasarımlı, basit ve bilgilendiricidir.
- İzlenen durumlarda değişiklik olunca otomatik alam üretir
- Pek çok bilgilendirme seçeneği vardır (Email, mobil telefon, SMS vs.)
- Sadece gerekli bilgileri gösterir.
- Kontroller kategorize edilebilir. Örneğin Ping çalışmıyor ise diğer servisler kontrol edilmez sadece sistemin çalışmadığı alarmı gönderilir.
- Kolayca genişletilebilir. Yeni servislerin kontrolü basit betikler ile yapılabilir. Tüm kontrollerin sadece tek bir satır bilgi döndürmesi yeterlidir.
- Büyük çapta kurumlara uyarlanabilir, ölçeklenebilir. Pek çok Unix'i destekler.

Neden Nagios Kullanmalı? -II-

- İzlenen host ve servisler için veri tabanı üzerinde kayıt geçmiş tutar.
- MRTG ile Host ve Servislere ait erişilebilirlik bilgilerini grafiklere dönüştürür.
- Değişik uçlardaki benzeri verileri birleştirerek grafiğe dönüştürebilir.
- Alarmları eskale edebilir.
- Alarmları kişilere veye gruplar bazında iletebilir.

Nagios Mimarisi

- Nagios basit bir kuruluma sahiptir.
- Nagios' un temel Yapısı:
  - Nagios sunucusunda çalışan Nagios daemon (*daemon*)
  - Nagios daemon üzerindeki kontrol betikleri (*check*)
  - Kontrol betiklerinin her biri kontrol edilen servisin durumuna dair bir sonuç döndürür (*status*)
  - Kontrol betikleri yerel sunucuda çalışır ve istenirse yerel servisleri istenirse uzak sistemlerdeki (*host*) servislerini sorgulayabililirler.
  - Eğer servisler uzktan sorgulanamıyor ise NRPE (NCSA) gerekebilir:
    - bazı servisler sadece local adrese bağlıdır.
    - Yerel firewall bazı portları güvenlik sebebiyle dışarı açmaz.

    Bu gibi durumlarda servislerin durumunu uzaktan sorgulamak mümkün olmamaktadır!

Nagios Mimarisi -II-

- Daemon – Nagios sunucu servisi
- Host – Ağ üzerinde çalışan ve kontrol edilecek bir ya da birden fazla servis çalıştıran bir bilgisayardır.
- Service – Bir host üzerinde çalışan ve kontrol edilemsini istediğiniz herhangibi programdır. Servisin durumu : OK, Warning, Critical ya da Unknown olabilir.
- Check – Sunucu üzerinde çalışan bir program ya da betiktir. Çıkış kodu servisin durumunu bildirir. Durum kodları 0,1,2 ya da -1 dir. (OK, Warning, Critical ve Unknown a karşılık gelir)
- Alert – Sunucuda çalışan servislerden birisinde bir hata oluşması drumunda tetiklenen ve çeşitli metodlarla belirlenen kullanıcıları haberdar eden mekanizmadır.

Nagios Bileşenleri

- Nagios Kaynak koddan derlenerek kurulabileceği gibi pek çok dağıtımın kendi paket yöneticisi ile de kurulabilmektedir.
- Nagios' un temel bileşenleri şunlardır:
  - Nagios – Sunucu yazılımı ve web bileşenleri
  - Nagios-Plugins – Nagios un sunucu ve servisleri izlemek için kullandığı kontrol betikleri
  - Nagios-NRPE – Betikleri uzak bir sistem üzerinde çalıştırmaya yarayan bileşeni. (Nagios Remote Plugin Executor)
  - NRPE' ye alternatif olarak üretilmiş olan NCSA. Ancak NCSA günümüzde NRPE kadar yaygın değildir.
  - Windows sunucuları denetlemek için NSClient++

Nagios Nasıl Kurulur ?

- Nagios'un çok fazla ön gereksinimi yoktur ancak şu paketlerin kurulmuş olması gereklidir:
  - Gd (PNG vw JPEG kütüphanleri GD ile kuruluyor),
  - gd-devel,
  - OpenSSL,
  - OpenSSL-devel,
  - MySQL (eğer MySQL log kullanılacaksa)
  - Net-SNMP-tools ve Net-SNMP-Utils (Eğer SNMP kullanılacasksa)
  - Fast-Ping (isteğe bağlı ancak oldukça faydalı)
  - Ekstradan izlenmesi gereken servisler için gerekli bileşenler ve bunların geliştirme kütüphaneleri (-devel sonekli paketleri). Örneğin PostgreSQL izlenecekse buna ait paketler.

Nagios Nasıl Kurulur ? -II-

- Öncelikle nagios'un çalışabilmesi için 2 adet grup eklenmesi gereklidir:
  - nagcmd (*groupadd nagcmd*)
  - nagios (*adduser nagios*)

  Bu gruplar eklenmezse ürün doğru çalışmayacaktır!
- Daha sonra nagcmd grubununun http ve nagios gruplarına eklenmesi gerekmektedir:

  /usr/sbin/usermod -a -G nagcmd nagios

  /usr/sbin/usermod -a -G nagcmd apache
- Son olarak http sunucusunu tekrar başlatarak grup ayarlarının etki olması sağlanmalıdır.

Nagios Nasıl Kurulur ? -III-

- Nagios sunucunun derlenmesi:

  tar xvzf nagios-x.y.z.tar.gz
  cd nagios-x.y.z
  ./configure –with-command-group=nagcmd –sysconfdir=/etc/nagios
  make all

- Değişik bileşenlerin kurulması:
  - *make install* (Sunucu Bileşenleri)
  - *make install-init* (Başlatma/durudurma/sorgulama betiği)
  - *make install-config* (Konfigürasyon dosyları)
  - *make install-commandmode* (PHP Betikleri)

Nagios Nasıl Kurulur ? -IV-

- Nagios Pluginlerinin derlenmesi:

```
tar xzf nagios-plugins-x.y.z.tar.gz
cd nagios-plugins-x.y.x
./configure
make all
make install
```

- Kurulum yapılırken bazen plugin bileşenlerinin yüklenmesi unutulabilmektedir. Bu durumda tüm kontrol edilme istenen servislerden 127 kodu alınır (127 – komut bulunamadı kodudur.) Böyle bir hata ile karşılaşıyorsanız derhal pluginleri kurun.

Nagios Nasıl Kurulur ? -V-

- Nagios' a web girişi için Şifre atanması:

  htpasswd -c /etc/nagios/nagios.pass magiosadmin

- Şifre dosyasının nagios apache dosyalarında tanımlanması gerekiyor

  .
  .
  AuthName "Nagios Access"
  AuthType Basic
  AuthUserFile /etc/nagios/htpasswd.users
  Require valid-user
  .
  .

- Bu işlemlerden sonra nagios başlatılmalı ve apache yeniden başlatılmalıdır.

NRPE Nasıl Kurulur ?

- Nagios Uzak Sistemlere NRPE kurulması
  - Gerekli bileşenler:
    - xinetd
    - OpenSSL, OpenSSL-devel
  - NRPE' nin derlenmesi:

```
tar xvzf nrpe-x.y.tar.gz
cd nrpe-x.y
adduser nagios
./configure --sysconfdir=/etc/nagios --enable-ssl --enable-command-args
make
make install
```

  - --enable-ssl anahtarı eklenmez ise NRPE bağlantısında “SSL Handshake Error” hatası alınır. Diğer bir alternatif de SSL'siz kullanımdır ancak SSL tabii ki daha güvenlidir.
  - --enable-command-args anahtarı NRP' ye paramtere geçirilmesine olanak tanır. Bu anahtar eklenmezse parametre olarak sadece komut adı geçirilir kontrol değerleri lokal olarak tanımlanmalıdır.

NRPE Nasıl Kurulur ? -II-

- Nagios Uzak Sistemlere NRPE kurulması
  - /etc/services dosyasına nrpe servisi eklenmesi:

    nrpe 5666/tcp #NRPE

  - Xinetd' ye servis eklemek

```
# default: on
# description: NRPE (Nagios Remote Plugin Executor)
service nrpe
{
        flags           = REUSE
        socket_type             = stream
        port            = 5666
        wait            = no
        user            = nagios
        group           = nagios
        server          = /usr/local/nagios/bin/nrpe
        server_args             = -c /etc/nagios/nrpe.cfg --inetd
        log_type        = SYSLOG local6
        log_on_failure          += USERID
        disable         = no
        only_from       = 127.0.0.1 10.0.0.1
}
```

NRPE Nasıl Kurulur ? -III-

- nrpe-x.y/sample_config dizinindeki nrpe.cfg dosyası /etc/nagios/nrpe.cfg oalrak kopyalanmalı ve içeriği gözden geçirilmelidir. (--sysconfdir parametresinin gösterdiği yer)

- Dosya sahibinini nagios olarak atamak gerekir.

  chown nagios.nagios /etc/nagios/nrpe.cfg

- Terminoloji: Nagios daki durumun tersine, istemcide çalışan NRPE sunucudur. Bu durumda Nagios server NRPE istemci üzerinden NRPE sunuculara bağlanmaktadır.

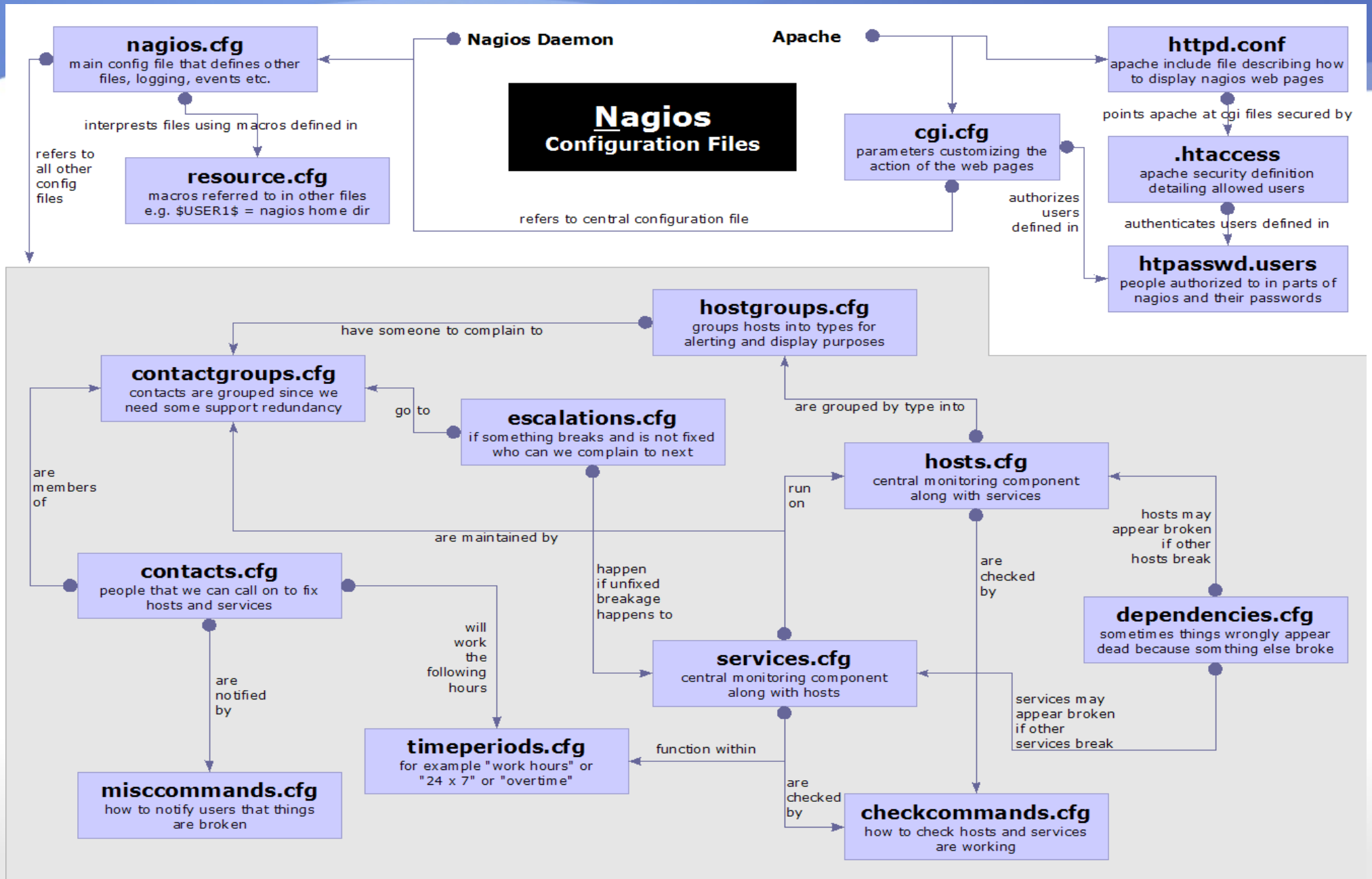
Nagios SELinux Notları

- Nagios ve SELinux:
  - SELinux mükemmel bir güvenlik uygulama sistemidir. Sistem yöneticilerinin , kullanıcıların dosya ve klasörlerine verdiği haklardan bağımsız olarak sistem üzerinde politika uygulayabilmelerine olanak verir.
  - Ancak henüz programcılar tarafından hak ettiği ilgiyi görememiştir. Pek çok programcı ilk iş SELinux'u kapatmayı önerir. Ancak SELinux ile birlikte çalışmak oldukça iyi bir fikiridir.
  - SELinux ayarları komutlara -Z anahtarı eklenerek görüntülenebilir. Örneğin ls, ps gibi pek çok komut SELinux ayarlarını görüntüler.
  - SELinux'u kullanmak için öncelikle /etc ve daha sonra Nagios Plugin klasöründeki dosyaların context leri değiştirilmelidir:

    chcon -R -t etc_t /etc/nagios
    chcon -R -t httpd_sys_script_rw_t /usr/local/nagios/var/rw/
    chcon -R -t httpd_sys_script_rw_t /usr/local/nagios/var
  - Daha sonra politika yaratılarak SELinux hatları buraya eklenebilir. Bir süre SELinux Permissive kipinde çalıştırılarak tüm politikaya aykırı işlemler belirlenebilir ve yeni bir politikaya dönüştürülebilir Daha sonra SELinux tekrar enforcing kipine alınabilir:

    grep AVC /var/log/audit/audit.log | audit2allow -M nagios
    semodule -i nagios

Nagios Konfigürasyon Dosyaları



Nagios Host

```
define host{
        host_name                       webserv01
        alias                           www.sunucum.com.tr
        address                         10.0.0.10
        check_command                   sunucu-ping-kontrol
        max_check_attempts              10
        check_period                    24x7
        notification_interval           120
        notification_period             24x7
        notification_options            d,r
        contact_groups                  unix-yonetici
        register                        1
        }
```

Nagios Service

```
define service{
        name                            sunucu-ping-kontrol
        service_description             PING
        is_volatile                     0
        check_period                    24x7
        max_check_attempts              4
        normal_check_interval           5
        retry_check_interval            1
        contact_groups                  unix-yonetici
        notification_options            w,u,c,r
        notification_interval           960
        notification_period             24x7
        check_command    check_ping!100.0,20%!500.0,60%
        hosts                           webserv01
        register                        1
        }
```

Nagios Check

```
#Kontrol Komutu
define command{
        command_name    host-ping-kontrol
        command_line    $USER1$/check_ping -H     $HOSTADDRESS$ -w 99,99% -c 100,100% -p 1
        }

# Parametresiz
# 'check_nrpe' command definition
define command{
        command_name    check_nrpe
        command_line    $USER1$/check_nrpe -H $HOSTADDRESS$ -c $ARG1$
        }

# Parametreli
# 'check_nrpe' command definition
define command{
        command_name    check_nrpe_parms
        command_line    $USER1$/check_nrpe -H $HOSTADDRESS$ -c $ARG1$ -a $ARG2$ $ARG3$
$ARG4$ $ARG5$
         }
```

Nagios Alert

```
define command{

        command_name    notify-by-email

        command_line    /usr/bin/printf "%b" "***** Nagios  *****\n\nNotification
    Type: $NOTIFICATIONTYPE$\n\nService: $SERVICEDESC$\nHost: $HOSTALIAS$\nAddress:
    $HOSTADDRESS$\nState: $SERVICESTATE$\n\nDate/Time: $LONGDATETIME$\n\nAdditional
    Info:\n\n$SERVICEOUTPUT$" | /bin/mail -s "** $NOTIFICATIONTYPE$ alert - $HOSTALIAS$/
    $SERVICEDESC$ is $SERVICESTATE$ **" $CONTACTEMAIL$

        }
```

Nagios Alert

```
define command{

        command_name    notify-by-email

        command_line    /usr/bin/printf "%b" "***** Nagios  *****\n\nNotification
    Type: $NOTIFICATIONTYPE$\n\nService: $SERVICEDESC$\nHost: $HOSTALIAS$\nAddress:
    $HOSTADDRESS$\nState: $SERVICESTATE$\n\nDate/Time: $LONGDATETIME$\n\nAdditional
    Info:\n\n$SERVICEOUTPUT$" | /bin/mail -s "** $NOTIFICATIONTYPE$ alert - $HOSTALIAS$/
    $SERVICEDESC$ is $SERVICESTATE$ **" $CONTACTEMAIL$

        }
```

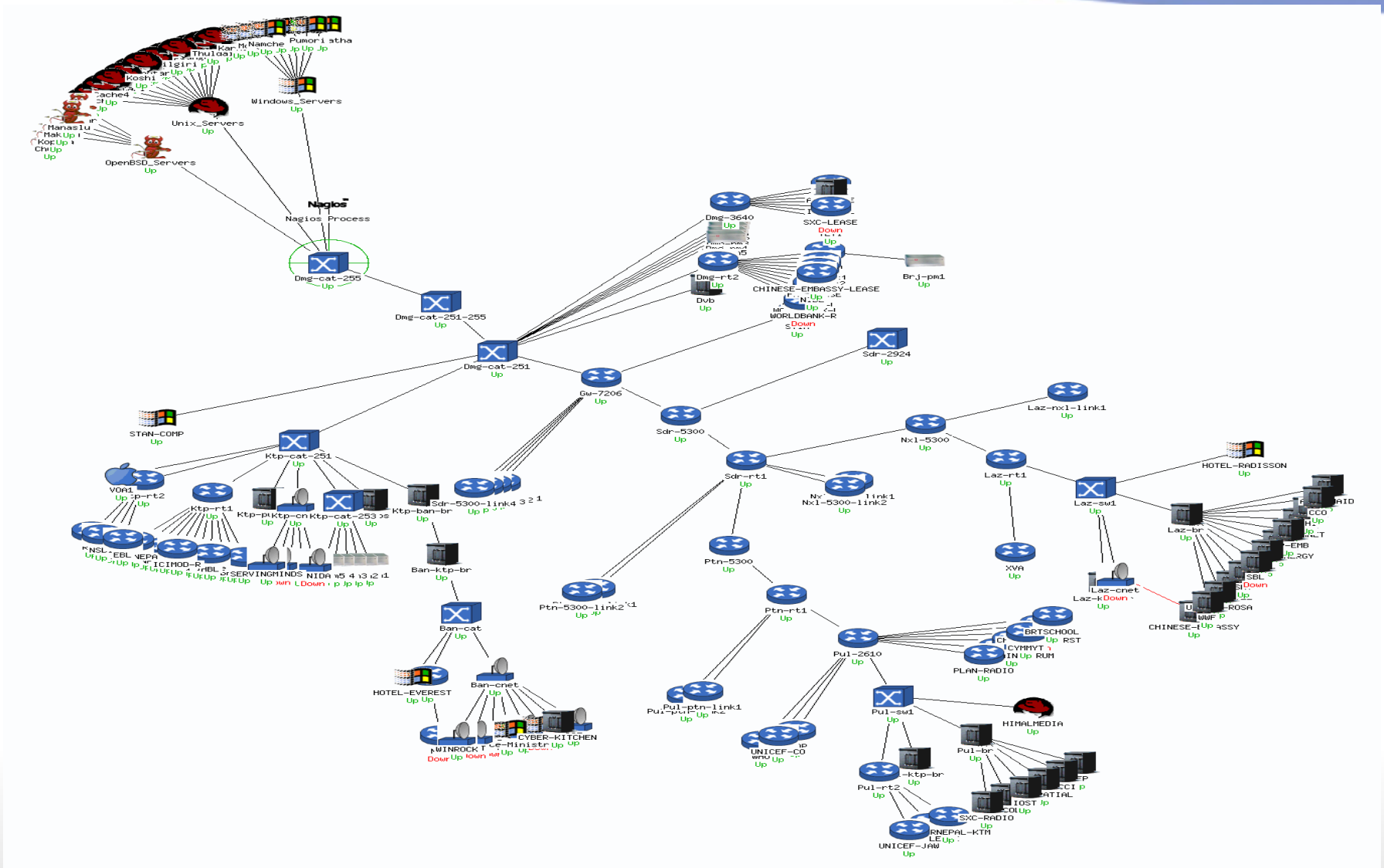
Nagios Plugin Geliştirme

```
#!/bin/bash
################################################################################################
# Name: check_xenvmk Plugin (c) 2009 by Kerem ERSOY GNU Public License V2.0
# Version: 1.0
# Exit Codes:
#      3 - Inderterminate Orange
#      2 - Critical Red
#      1 - Warning Yellow
#      0 - OK Green
# Notes:
# - For successful operation of the plugin edit your /etc/sudoers with visudo
#   - Comment: Defaults    requiretty
#   - Add    : nagios          ALL=(ALL)       NOPASSWD: /usr/sbin/xm list
################################################################################################
if [ -z $4 ]; then

   echo "usage $(basename $0) -w [num] -c [num]"
   exit 3
fi
LISTDOMU=$(sudo /usr/sbin/xm list | egrep -v "^Na|^Do" | cut -f1 -d" " | xargs)
NUMDOMU=$(echo $LISTDOMU | wc -w)
if [ $NUMDOMU -le $4 ]; then
   echo "Critical Number of DomUs ($NUMDOMU) is less than cirtical value $4"
   exit 2
fi

if [ $NUMDOMU -le $2 ]; then
   echo "Warning Number of DomUs ($NUMDOMU) is less than the warning value $2"
   exit 1
fi
echo "OK Dom0 $(hostname) is running $NUMDOMU DomU : $LISTDOMU"
exit 0
```

Nagios Host Ekranı

Nagios Harita Ekranı

Nagios Kurumsal Harita Ekranı

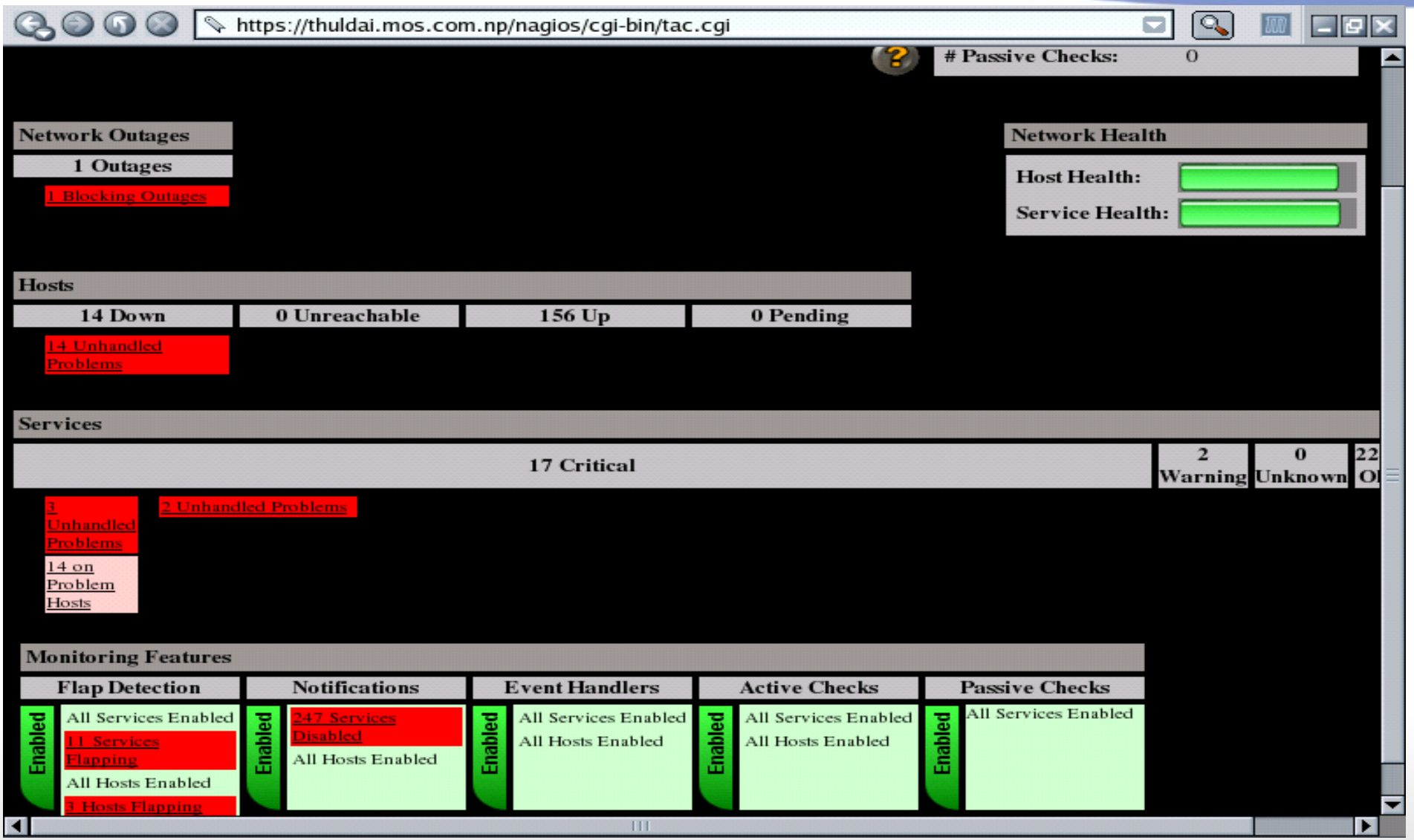


Nagios Servisler Ekranı

Nagios Özet Durum Ekranı

Nagios Detaylı Durum Ekranı

Nagios Taktik Ekranı

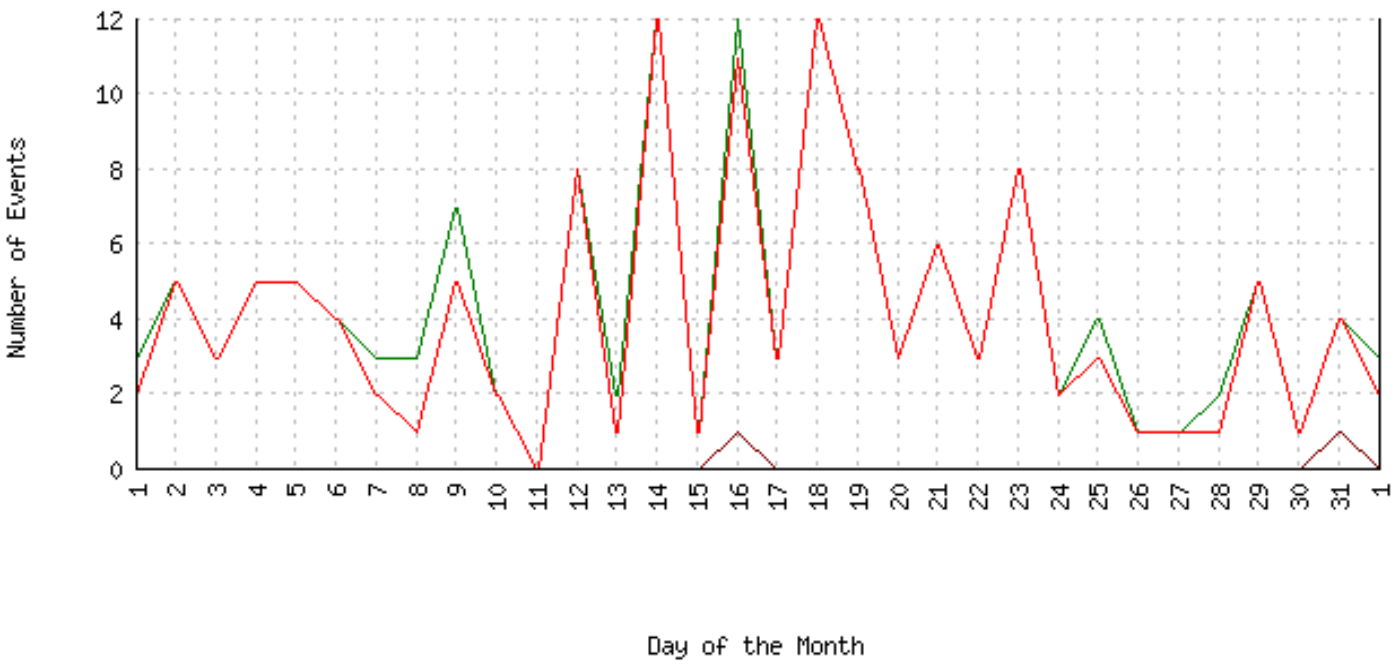


Nagios Histogram Ekranı

Histogram

Event History For Host 'Don_Bosco'

Thu Jan 1 00:00:00 2004 to Sun Feb 1 00:00:00 2004



EVENT TYPE	MIN	MAX	SUM	AVG
Recovery (Up):	0	12	138	4.45
Down:	0	12	128	4.13
Unreachable:	0	1	2	0.06

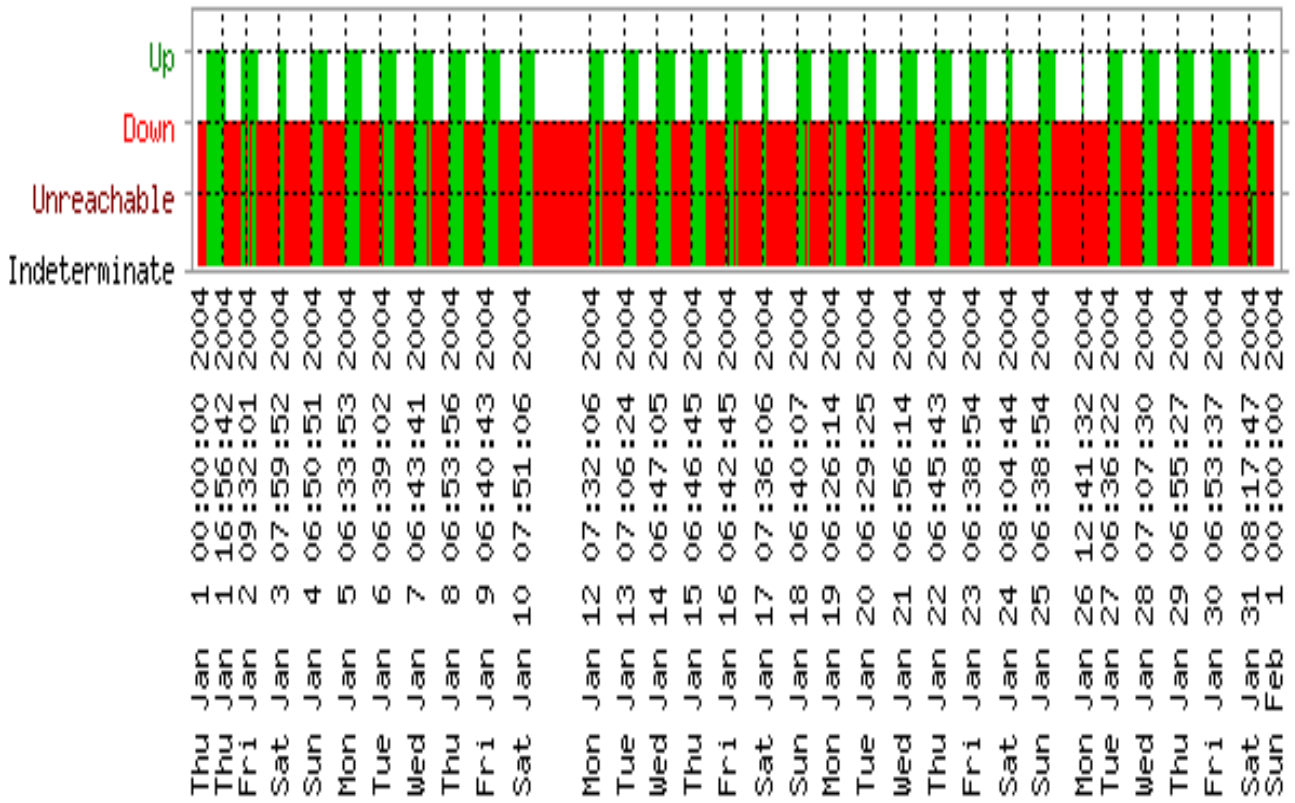
Report Produced By:
Nagios®
http://www.nagios.org

Nagios Host Trend Ekranı

Trends

State History For Host 'Don_Bosco'

Thu Jan 1 00:00:00 2004 to Sun Feb 1 00:00:00 2004

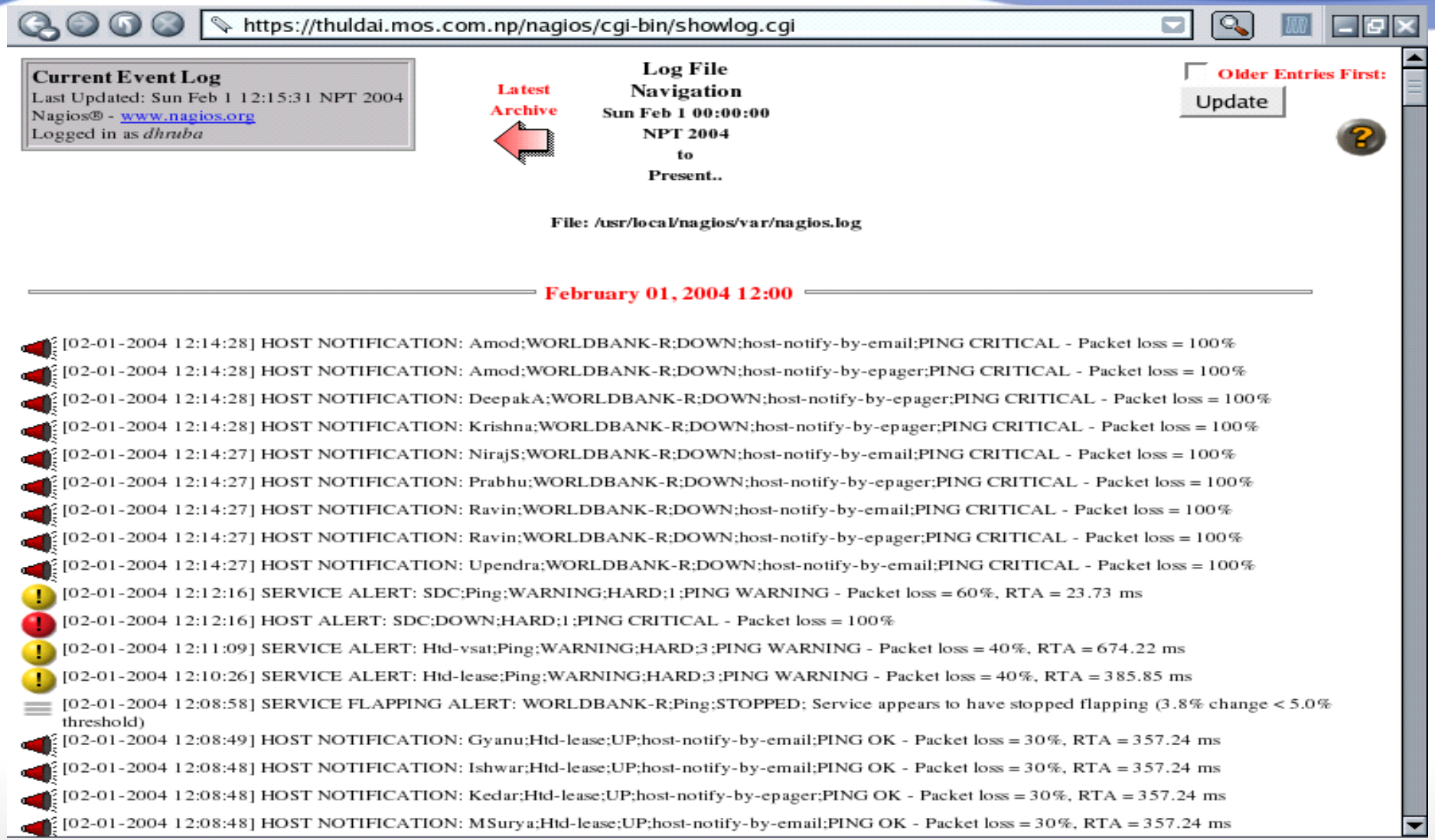


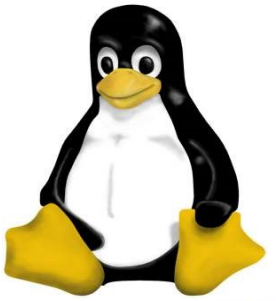
State Breakdowns:

Up	: (32.6%)	10d 2h 21m 41s
Down	: (67.1%)	20d 19h 17m 27s
Unreachable	: (0.3%)	0d 2h 5m 12s
Indeterminate	: (0.0%)	0d 0h 15m 40s

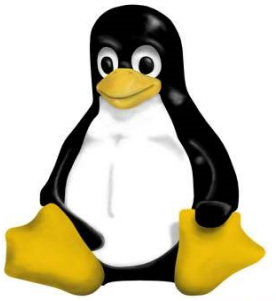
Report Produced By:
Nagios®
http://www.nagios.org

Nagios Log Ekranı





Soru-Cevap



Teşekkürler !