Syslog Server

Syslog, cihazlar üzerinde meydana gelen olayların/değişimlerin kayıt altına alınarak incelenebilmesini sağlayan protokoldür. Networkte kullandığımız router ve switch gibi cihazlar da bu protokolü desteklemektedir. Bu sayede networkte bir problem oluştuğunda cihazlar üzerinde oluşan loglar incelenerek problemin kaynağı çok daha hızlı tespit edilebilmektedir.

Cihazlar üzerinde oluşan loglar cihaz üzerinde depolanabildiği gibi uzak bir Syslog sunucusu üzerinde de depolanabilmektedir. Bu işlem için UDP 514 portu kullanılmaktadır.

Varsayılanda cihaz üzerinde gerekli gereksiz her şey loglanmaktadır. Bu durum gereksiz kaynak tüketimine neden oluyor. Bu nedenle cihazlar üzerinde özelleştirmeler yapılarak kayıt altına alınması istenen durumların belirlenmesi gerekiyor. Bu süreci daha kolay yönetebilmek için sistem üzerinde oluşan her bir durumu 7 önem seviyesinden biriyle eşlenmektedir. Bu önem dereceleri;

Severity Level	Level Name	Description
0	Emergencies	System unusable
1	Alerts	Immediate action needed
2	Critical	Critical conditions
3	Errors	Error conditions
4	Warnings	Warning conditions
5	Notifications	Normal but significant conditions
6	Informational	Informational messages only
7	Debugging	Debugging messages

- Severity Level 0 –4 , cihaz üzerindeki yazılım veya donanım arızalarıyla ilgili hata mesajlarıdır. Cihazın işleyişinde bir sorun olduğunu göstermektedir. Önem seviyesi ise durumun ciddiyetini göstermektedir.
- Severity Level 5, önemli olaylar için oluşturulan kayıtlardır. Örnek olarak bir arayüzün açılması veya kapatılması, cihazın yeniden başlatılması gibi olaylar verilebilir.
- Severity Level 6, cihazın işleyişini etkilemeten bilgilendirme mesajlarıdır. Örnek olarak cihazlar acılırken konsola çıkarılan mesajlar verilebilir.
- Severity Level 7, cihaz üzerinde gerçek zamanlı olarak herhangi bir hata veya trafik mesajı hakkında bilgi alabilmek için debug komutu kullanılmaktadır. Debug modunda oluşan olaylar için oluşturulan mesajlardır. Örnek olarak "**debug ip icmp**" komutuyla cihaza ping paketi geldiğinde kayıt altına alınması sağlanabilir.

Oluşturulan kayıtlarda, kaydın hangi birim tarafından oluşturulduğunu ifade etmek için belirli kısaltmalar (%facility) bulunmaktadır. Bu kısaltmalarda birkaçına örnek olarak;

- IF – kaydın bir arayüz tarafından oluşturulduğunu gösterir.
- IP – kaydın bir IP tarafından oluşturulduğunu gösterir.
- OSPF - kaydın OSPF protokolü tarafından oluşturulduğunu gösterir.
- SYS - kaydın işletim sistemi tarafından oluşturulduğunu gösterir.
- IPSEC - kaydın IPSEC protokolü tarafından oluşturulduğunu gösterir.

verilebilir. Varsayılanda syslog mesaj formatı aşağıdaki gibidir;

```
%facility-severity-MNEMONIC: description
```

```
*Mar  1 00:16:26.719: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
*Mar  1 00:16:27.719: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
```

Syslog Konfigürasyonu

- Varsayılanda cihazda oluşturulan loglara tarih ve saat bilgileri eklenmemektedir. Bu durumda oluşan değişimlerin zaman bilgileri tanımlanamayacaktır. Oluşturulan loglara zaman damgası eklenebilmesi için "**service timestamps log datetime**" komutu kullanılıyor.
    - Bu komut kullanılmadan önce cihaz üzerindeki saat ve tarih bilgilerinin günvel oluğ olmadığı kontrol edilmelidir.
- Cihaz üzerinde oluşan logların gönderileceği Syslog sunucusunun ip adresi "**logging host <Ip Address | hostname>"** komutuyla tanımlanıyor.
- Oluşan logların önem seviyeleri dikkate alınarak Syslog sunucusuna gönderilmesi sağlanabiliyor. Bunun için "**logging trap <Level>**" komutu kullanılarak hangi önem seviyesinden ihtibaren kayıt altına alınması gerektiği belirlenebiliyor.
    - Örnek olarak "logging trap 5" komutu Severity Level 5 ve daha alt seviyedeki (5,4,3,2,1) logların kayıt altına alınması sağlanabiliyor.
- İsteğe bağlı olarak Syslog sunucusuna belirli bir arayüzden gönderilmesi saplanabiliyor. Bunun için "**logging source-interface <Interface ID>**" komutu kullanılıyor.
- Syslog protokolü varsayılanda devrededir ama her ihtimale karşı (devre dışı bırakılma ihtimaline karşı) "**logging on**" komutuyla devreye alınabilir.

```
R1(config)#service timestamps log datetime
R1(config)#logging host 192.168.10.100
R1(config)#logging trap 5
R1(config)#logging source-interface fa 0/0
R1(config)#logging on
```

Temel konfigürasyon sonrasında isteğe bağlı olarak özelleştirmeler yapılabilmektedir https[:]//www.cisco.com/c/en/us/td/docs/routers/access/wireless/software/guide/SysMsgLogging.html.

```
R1(config)#logging ?
  Hostname or A.B.C.D  IP address of the logging host
  buffered             Set buffered logging parameters
  buginf               Enable buginf logging for debugging
  cns-events           Set CNS Event logging level
  console              Set console logging parameters
  count                Count every log message and timestamp last occurrence
  discriminator        Create or modify a message discriminator
  dmvpn                DMVPN Configuration
  esm                  Set ESM filter restrictions
  exception            Limit size of exception flush output
  facility             Facility parameter for syslog messages
  filter               Specify logging filter
  history              Configure syslog history table
  host                 Set syslog server IP address and parameters
  message-counter      Configure log message to include certain counter value
  monitor              Set terminal line (monitor) logging parameters
  on                   Enable logging to all enabled destinations
  origin-id            Add origin ID to syslog messages
  persistent           Set persistent logging parameters
  queue-limit          Set logger message queue size
  rate-limit           Set messages per second limit
  reload               Set reload logging level
  server-arp           Enable sending ARP requests for syslog servers when
                       first configured
  source-interface     Specify interface for source address in logging
                       transactions
  trap                 Set syslog server logging level
  userinfo             Enable logging of user info on privileged mode enabling
```

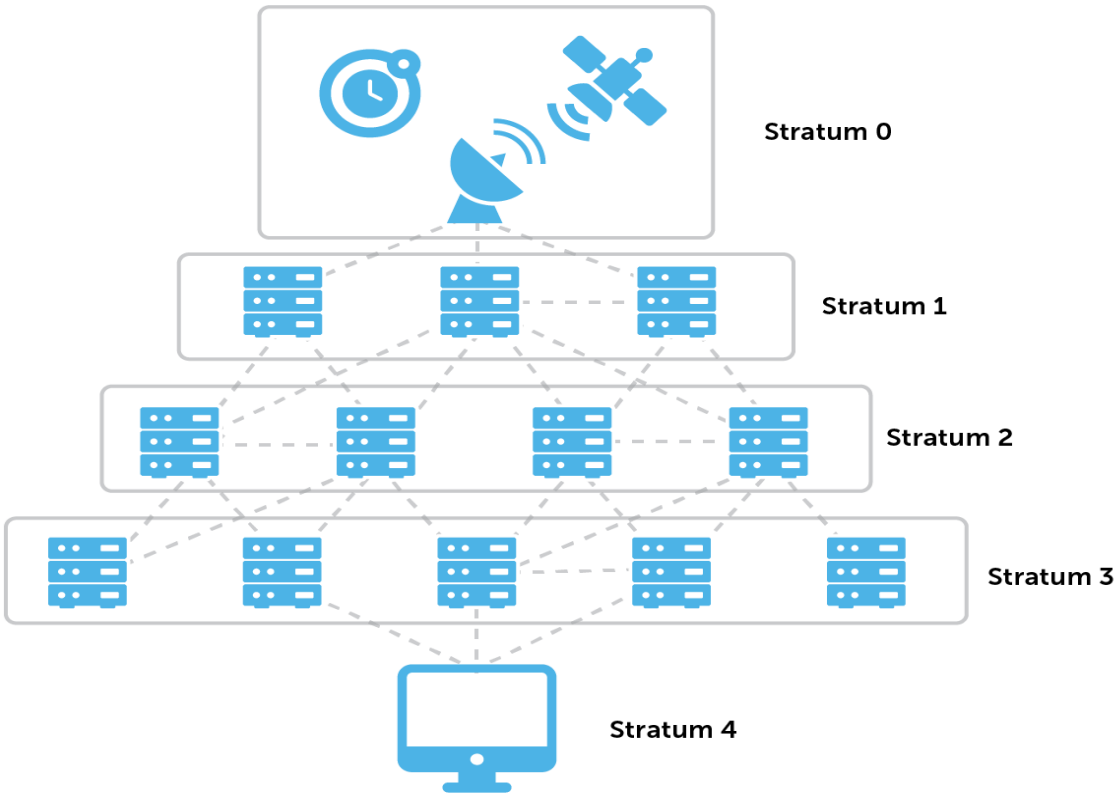
NTP Server

NTP protokolü, hem saat hem de tarih bilgileri network cihalarına öğretmek için kullanılan bir protokoldür. UDP 123 portunu kullanır. Networkte kullanılan cihazların hepsinde saat ve tarih bilgileriin aynı olması gerekiyor. NTP sunucuları kullanılarak da networkteki bütün cihazların saat ve tarih bilgilerinin senkronize edilmesini sağlayan protokoldür.

Cihazların tarig ve saat bilgisi daha çok log takibi (throubleshooting yaparken veya anomali tespitinde loglarda bulunan zaman damgaları önemli oluyor) yapılacağı zamanlarda önem kazanıyor.

NTP protokolü hiyerarşik/katmanlı bir yapıdadır. Bu hiyerarşinin en tepesinde bulunan cihaz Stratum 0 oluyor. Bir cihazın Stratum 0'a olan uzaklığı o cihazın hangi katmanda oldupunu tanumlar.

- Stratum 0 en yetkili zaman kaynağını sağlayan bir cihazı tanımlar. Bu cihazlara örnek olarak atomik ve GPS saatleri örnek verilebilir. Gecikmenin düşük, hassasiyetin yüksek olduğu zaman tutma cihazları olarak da tanımlanabilirler.
- Stratum 1, Stratum 0'a 1 hop uzaklıktaki cihazlardır.



Kurum ciharlarına saat ve tarih bilgileri tanımlamanın birçok yöntemi vardır. Bunlar;

- Kurumlarda bir NTP sunucusu kurularak topolojideki bütün cihazların bu sunucu üzerinden tarih ve saat bilgisi alması sağlanabiliyor.
- Topolojide bir cihaza NTP sunucusunda (uzak bir NTP sunucusu olabilir) tarih ve saat bilgisi aldırılarak cihaz üzerinde NTP Server hizmeti devreye alınıyor. Topolojideki diğer cihazlar da bu cihaz üzerinden (NTP Sunucu hizmeti veren cihaz) tarih ve saat bilgilerini set edebiliyorlar.
- Cihazlardan birinde tarih ve saat bilgisi manuel olarak tanımlanıyor. Aynı zamanda cihaz üzerinde NTP Server hizmeti devreye alınarak topolojideki diğer cihazların bu cihaz üzerinden tarih ve saat bilgisi alması sağlanabiliyor.

Tarih ve Saat Konfigrasyon

- Saat ve tarih bilgilerini manuel olarak tanımlamak için "**clock set <hh:mm:ss dd:MM:yyyy>**" komutu kullanılıyor.

```
R1#clock set 14:00:00 16 dec 2022
R1#
*Dec 16 14:00:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 00:04:20 UTC Fri Mar 1 2002 to 14:00:00 UTC Fri
 Dec 16 2022, configured from console by console.
```

- Bölge seçimi yaparak saat bilgisi alması için "**clock timezone <TimeZone>**" komutu kullanılıyor (TimeZone, https[:]//fastreroute.com/cisco-clock-timezone-configuration/).

```
R1(config)#clock timezone trt +3
R1(config)#
Dec 16 14:20:40.307: %SYS-6-CLOCKUPDATE: System clock has been updated from 17:20:40 trt Fri Dec 16 2022 to 17:20:40 trt Fri
 Dec 16 2022, configured from console by console.
```

  - Saat ve tarih tanımlamaları için özelleştirmeler de yapılabiliyor. (Detaylar, https[:]//www.cisco.com/c/en/us/support/docs/smb/switches/cisco-small-business-300-series-managed-switches/smb5584-configure-system-time-settings-on-a-switch-through-the-comma.html)

```
R1(config)#clock ?
  initialize   Initialize system clock on restart
  save         backup of clock with NVRAM
  summer-time  Configure summer (daylight savings) time
  timezone     Configure time zone
```

- NTP sunucusundan ip alabilmesi Global konfigürasyon modundan "**ntp server <NTP Server Ip Address**>" komutu kullanılıyor.

```
R2(config)#ntp server 10.0.0.1
```

- Cihazlarda NTP server hizmeti devreye alınmak isteniyorsa "**ntp master <Stratum Level>**" komutu kullanılıyor.
  - NTP Server hizmeti devreye alınan cihazda saat bilgisi manuel olarka girilmişse ve komut içerisinde Stratum değeri belirtilmemişse Stratumm değeri varsayılanda 8 olarak tanımlanıyor.

```
R3(config)#ntp ?
  access-group        Control NTP access
  authenticate        Authenticate time sources
  authentication-key  Authentication key for trusted time sources
  broadcastdelay      Estimated round-trip delay
  clock-period        Length of hardware clock tick
  logging             Enable NTP message logging
  master              Act as NTP master clock
  max-associations    Set maximum number of associations
  peer                Configure NTP peer
  server              Configure NTP server
  source              Configure interface for source address
  trusted-key         Key numbers for trusted time sources

R3(config)#ntp master ?
  <1-15>  Stratum number
  <cr>
```

|→ Örnek uygulama için Lab->Çalışma dizinine bakabilirsin.

Cihazlarda tarih ve saat bilgileri manuel olarka tanımlandığında Stratum değeri 16 olarak tanımlanmaktadır. Bu doğrultuda NTP protokolünde cihazların kaynağa (Stratum 0) uzaklığı en fazla 15 hop/birim olabiliyor.

Kontrol Komutları

- sh logging
- sh ntp assıciated
- sh ntp status
- sh clock detail
- sh clock