

## Cisco Cihazlarda Konfigürasyon Değişikliklerinin İzlenmesi ve Loglanması (Configuration Change Notification and Logging) Sınmaz KETENCİ – İTÜ/BİDB 2010

Sorumlu olduğunuz ve yönettiğiniz network'ün sınırları genişledikçe herhangi bir cihazda yapılan bir konfigürasyon değişikliğinin network'te beklenmedik problemlerin ortaya çıkma olasılığını yükselttiğini söyleyebiliriz. Bunun yanında bu yapılan konfigürasyon değişikliğini de siz yapmadıysanız yandınız:) Problem yetmiyormuş gibi bir de “yapılan değişiklik nedir?”in cevabını aramak çıktı! Eğer network yöneticileri kişisel kullanıcı adları ile cihazlara login oluyorsa o kişiye ulaşım yaptığı değişikliği öğrendikten sonra problemin nedenini yorumlamak mümkün olacaktır.

Belli aralıklarla cihazların konfigürasyon yedeklerini alan ve bunlar arasındaki farklılıklardan yapılan konfigürasyon değişikliklerini gösteren Ağ Yönetim Yazılımları(NMS) var. Ayrıca harici bir TACACS+ sunucusu kullanarak da cihazlar üzerinde yürütülen tüm komutların loglanması sağlanabilir. Fakat bu seçenekler, ücretli yazılımlar için maliyet ya da açık kaynak kodlu yazılımlar için ise ekstra bilgi ya da zaman gerektiriyor. Bu seçeneklerin network'te uygulanmasına geldiğinde çoğunlukla yapılacaklar listesine eklemekten öteye geçmiyor☺

Aslında uzun yıllardır Cisco cihazlarımızın içinde yatan aslanı uyandırma vakti geldi de geçiyor! Cisco IOS **Configuration Change Notification and Logging** özelliği ile yapılan konfigürasyon değişikliklerine yol açan komutları, kimin ne zaman yürüttüğü bilgisini loglayabiliyor. Varsayılanda bu özellik kapalı durumda. Devreye alındığında cihaz kendi üzerinde yürütülen son 100 konfigürasyon komutu için belirttiğimiz bilgileri logluyor. İstenirse bu logların syslog'a iletilmesi de sağlanıp harici bir syslog sunucusunda değişiklikleri saklamak mümkün ki yapılması gereken de bu olmalı. Bu özelliğin desteklenebilmesi için cihazınızın **12.3(4)T, 12.2(25)S, 12.2(27)SBC, 12.2(33)SRA, 12.2(33)SXH, 12.2(33)SB** IOS'lar ve sonrasındaki versiyonlarından platformuna uygun bir tanesine sahip olması gerekiyor. Yaygın olarak kullanılan cihazlara göz atarsak, 2950 serisi için yazının yazıldığı tarihteki son IOS versiyonu **12.1(22)EA13** dolayısı ile bu özellik desteklenmiyor. Fakat iyi haber, son 4-5 yıl içinde IOS upgrade yapılan router'ların ve tüm 2960 serisi switchlerin bu özelliği desteklemesidir.

Gelelim konfigürasyona ve sonuçlarını gözlemlemeye, konfigürasyon oldukça basit. Bu özelliği devreye alırken de bir konfigürasyon değişikliği yaptığımızdan ilk meyvelerini oldukça çabuk toplayacağız☺

```
Agciyiz.net#conf t
Agciyiz.net(config)#archive
Agciyiz.net(config-archive)#log config
Agciyiz.net(config-archive-log-cfg)#logging enable
Agciyiz.net(config-archive-log-cfg)#end
```

Varsayılan ayarları ile devreye aldık. **show archive log config all** komutu ile tüm loglanan komutları görüntülemek mümkün. Tüm komutların dışında belli bir kullanıcının girdiği komutları da görüntüleyebilirsiniz.

**Agciyiz.net#show archive log config all**

```
idx  sess      user@line  Logged command
  1   1    agciyiz@vty1 | logging enable
```

Şimdi admin1 ve admin2 kullanıcılarını yerel olarak ekleyelim.

**Agciyiz.net#conf t**

```
Agciyiz.net(config)#username admin1 secret sifre111
Agciyiz.net(config)#username admin2 secret sifre222
Agciyiz.net(config)#end
```

**Agciyiz.net#show archive log config all**

```
idx  sess      user@line  Logged command
  1   1    agciyiz@vty1 | logging enable
  2   2    agciyiz@vty1 |username admin1 secret sifre111
  3   2    agciyiz@vty1 |username admin2 secret sifre222
```

Yukarıdaki çıktıdan da görebildiğimiz gibi konfigürasyon komutları loglanırken girdiğimiz şifreler de loglanıyor. Bunu engellemek için **configuration change logger configuration** mode'da **hidekeys** komutunu girmemiz gerekiyor.

**Agciyiz.net(config)#archive**

```
Agciyiz.net(config-archive)#log config
Agciyiz.net(config-archive-log-cfg)#hidekeys
Agciyiz.net(config-archive-log-cfg)#end
```

**Agciyiz.net#conf t**

```
Agciyiz.net(config)#username admin3 secret sifre333
Agciyiz.net(config)#end
Agciyiz.net#show archive log config all
```

```
idx  sess      user@line  Logged command
  1   1    agciyiz@vty1 | logging enable
  2   2    agciyiz@vty1 |username admin1 secret sifre111
  3   2    agciyiz@vty1 |username admin2 secret sifre222
  4   3    agciyiz@vty1 |archive
  5   3    agciyiz@vty1 | log config
  6   3    agciyiz@vty1 | hidekeys
  7   4    agciyiz@vty1 |username admin3 secret *****
```

Bunun yanında en önemli özelliği olarak sayabileceğimiz bu logların syslog'a iletilebilmesi ve harici bir syslog sunucusunda cihazlarımız üzerindeki tüm konfigürasyon komutlarının kayıt altında tutulabilmesi. Bunu **notify syslog** komutu ile sağlayabiliyoruz.

```
Agciyiz.net(config)#archive
Agciyiz.net(config-archive)#log config
Agciyiz.net(config-archive-log-cfg)#notify syslog
```

\*\*\***notify syslog** komutu ile sadece syslog'a logların iletilmesini sağlar. Komutların harici bir syslog sunucusuna iletilmesi isteniyorsa global configuration mode'da "**logging <syslog\_ip\_adresi>**" komutunun girilmiş olması gerekir.

```
Agciyiz.net#show logging
```

...

```
Jun 6 15:12:01: %PARSER-5-CFGLOG_LOGGEDCMD: User:agciyiz logged
command:notify syslog
```

Son olarak cihaz üzerinde tutulacak komut sayısının varsayılanda 100 olduğundan bahsetmiştik. Bu sayı 1 ile 1000 arasında ayarlanabiliyor. Biz bu sayıyı 250 olarak ayarlayalım.

```
Agciyiz.net(config-archive-log-cfg)#logging size 250
```

Yaptığımız tüm konfigürasyonu özetlemeyi ise **Configuration Change Notification and Logging** özelliğinin show komutu çıktısına bırakıyoruz:)

```
Agciyiz.net#sh archive log config all
```

idx	sess	user@line	Logged command
1	1	agciyiz@vty1	logging enable
2	2	agciyiz@vty1	username admin1 secret sifre111
3	2	agciyiz@vty1	username admin2 secret sifre222
4	3	agciyiz@vty1	archive
5	3	agciyiz@vty1	log config
6	3	agciyiz@vty1	hidekeys
7	4	agciyiz@vty1	username admin3 secret *****
8	5	agciyiz@vty1	archive
9	5	agciyiz@vty1	log config
10	5	agciyiz@vty1	notify syslog
11	5	agciyiz@vty1	logging size 250

Bu özelliği devreye alırken herhangi özel bir parametre girilmiyor, uğraşmadan tüm cihazlara copy-paste yapalım diyorsanız hiç durmayın derim;

```
conf t
archive
log config
logging enable
logging size 250
notify syslog
hidekeys
```